电脑系列丛书

电脑病毒防治快易通

张保田 编

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

一学就会
一点就通

操作

它代表着此段文字是操作的重点，千万注意，一定要认真操作

警告

它代表着使用者在此处可能会犯致命性的错误，可要小心噢！

步骤

它代表着此处是操作的具体步骤，您可按此法轻松完成你要做的事情

说明

它代表着此段文字是重点说明，提醒您认真阅读

参见

当您偶而忘记或很久没有用而生疏某些问题时，此处为您提供查询线索

范例

它代表着您可以通过此例，验证您是否真正掌握了该有的重点

提示

它代表您要注意的问题，防止您掉入一般常见的错误陷井里

ISBN 7-5053-3455-7

9 787505 334557 >

ISBN7-5053-3455-7/TP·1362

定价：10.00 元

快易通电脑系列丛书

电脑病毒防治快易通

张保田　编

電子工業出版社

内 容 提 要

本书对于病毒的基本知识、结构、机理、种类以及防反病毒的原理、产品给出了比较详细的描述和分析，对于一些常见的热点问题也给出了详细解答。对于计算机用户更好地保护自己的资源免受病毒侵害提供了很好的帮助。

本书用于计算机用户，病毒防治与研究的技术人员等参考。

快易通电脑系列丛书

电脑病毒防治快易通

张保田 编

责任编辑：吴 源

特约编辑：李海鹏

*

电子工业出版社出版

北京市海淀区万寿路 173 信箱 (100036)

电子工业出版社发行 各地新华书店经销

电子工业出版社计算机排版室排版

北京市顺义县天竺颖华印刷厂印刷

*

开本：850 × 1168 毫米 1/32 印张：4.75 字数：127.6 千字

1996 年 8 月第一版 1996 年 8 月第一次印刷

印数：8000 册 定价：10.00 元

ISBN 7-5053-3455-7/TP · 1362

总　序

微型计算机(又称微电脑)的诞生,使人人用电脑成为现实。"信息高速公路"在全球的迅猛发展,网络对世界的"链接"与"并轨",将个人、家庭、企业与国家连成一体,使我们的世界变成了小小的地球村。一个全民学电脑、用电脑的深层次的普及已在我国兴起,并已成为提高劳动者素质,实现我国经济发展和科技进步的重要保证。

但是如何使用电脑,用好电脑,使电脑真正成为随心所欲的好帮手,则是广大群众所迫切需要了解和掌握的。

本套丛书就是这一背景下,由电子工业出版社、北京软件行业协会、中国电脑教育报、电脑爱好者杂志社,聘请国内计算机专家、教授、科普工作者精心策划编写的一套面向全民的计算机普及读物。丛书选材软硬件兼顾,硬件环境着重于目前的主流微型计算机;软件尽量采用最新版本。快!易!通!体现了本丛书的最大特点。

快:《丛书》选材安排以"少而精"为原则,使读者在最短的时间内学到最基本也是最精华的知识。

易:《丛书》内容介绍上力求生动活泼、图文并茂、幽默风趣。对于专业术语及技术的论述,强调由浅入深,通俗易懂,尽量用生活化、拟人化的语言进行叙述。

通:《丛书》内容选择突出"实用性",即一本书介绍一个实际应用技术,学了就能用,内容重点在于使用与操作步骤。

《丛书》从书面编排、版式设计、标题结构、开本大小上也都突出了创意新颖的特点。

本《丛书》的读者对象是:在校的中小学生及家长;为适应形势而需要学习电脑的各类人员;电脑爱好者、使用者、自学者;各种短训班学员以及各年龄结构、各种职业的人士。

本丛书是打开计算机殿堂的入门钥匙,以其实用、精炼、活泼、耐

读、新颖为宗旨，满足人们快节奏生活和学习电脑的愿望，消除人们对电脑的恐惧感、神秘感，使读者尽快地进入电脑这个神奇而又使人仰目的乐园。

“电脑插上就能用”这一口号已成现实；

“信息垂手即可行”这一目标已在眼前；

“从书开卷便有益”这一愿望已经出现。

愿本丛书能成为你进入电脑世界最好的伙伴！

本套丛书的编写得到了各方面人士的大力协作，特别是北京市“三金”领导小组办公室（筹）华平澜主任的支持。在丛书的征名中，得到近千人的推荐，最后我们选中了江超和武俊车二位同志举荐的《快、易、通电脑系列丛书》为名，在此一并致谢！

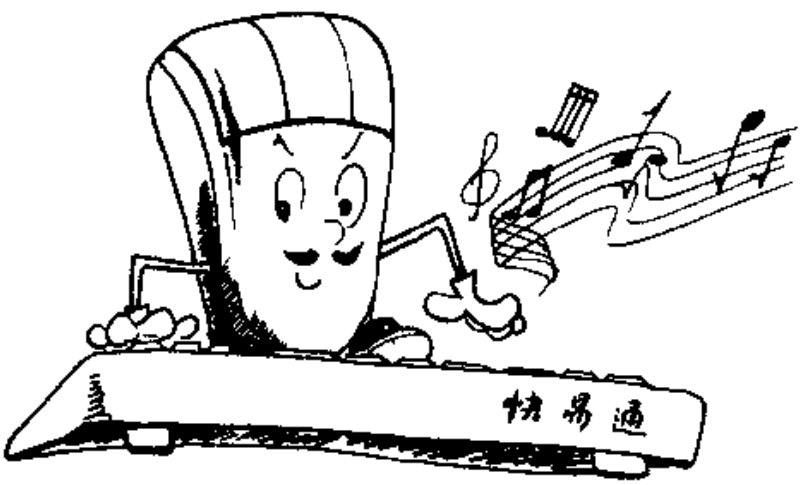
主编　朱继生

1995.9.9

目　录

第一章

计算机病毒的基本知识



在所有计算机软件中，有一类软件最不受欢迎，那就是计算机病毒。幽灵、黑色星期五、磁盘杀手……它们用不着用户去刻意收集，恰恰相反总是千方百计背着用户钻进计算机系统潜伏、传染、激发、破坏。每一位用户都憎恶病毒，却不得不同病毒打交道。

什么是计算机病毒？

怎样防止病毒进入自己的微机系统？

微机万一感染了病毒怎么办？

本书将为用户解答这些问题。

1.1 生物病毒与计算机病毒

病毒一词源于生物学，生物病毒由核酸分子构成，而核酸分子又由四种基本的核苷酸连结而成。核苷酸的排列顺序决定了生物的遗传密码。生物病毒在一定条件下侵入生物细胞，感染了病毒的细胞就成为病毒的"宿主"，病毒在宿主中潜伏、发作、自我复制、再传染……

与生物病毒类似，计算机病毒是一种人为编制的，能够自我复制的计算机程序。病毒的自我复制，也就是通常所说的传染，是在违背用户意愿情况下隐蔽进行的。病毒通过传染可能扩散侵入很多计算机系统，当某种条件被满足时破坏微机的信息资源，给用户造成巨大损失。很多病毒具有明显的破坏作用，但也有些病毒只是单纯地传染。不论是否有明显的破坏行为，只要一个程序在非用户授权情况下进行传染扩散，它就是计算机病毒。

每一个计算机病毒的原始程序都是人为编制的，通常病毒编制者是了解微机原理和操作系统的人，他们设计一段病毒程序，以手工操作的方式把病毒程序"嫁接"到正常磁盘上向外扩散。比方说病毒编制者可以在学校的公用计算机上使用他所炮制的含毒软件，由于病毒具有传染性，会使公用计算机上的很多软件都染上病毒。其他上机者从公用计算机拷贝出带毒软件拿到别的计算机系统使用，病毒会再传染其他系统……这样病毒就以一传十，十传百的树形结构不断传播扩散。

如果人们不能及时发现消除病毒，那么在某种特定条件下，染上病毒的计算机的信息系统会同时被破坏。

计算机病毒的形成有着久远的历史。早在半个世纪以前，伟大的数学家和计算机科学家冯·诺依曼就提出了复杂机械的自动复制理论，也就是计算机程序能够在内存中自我复制。50年代，著名的美国电报电话公司贝尔实验室的一些年轻研究人员热衷于一种他们自己创造的游戏，玩法是每人编制一段小程序去攻击对方的程序，赢家当然是毁灭对方程序者。这种会引起计算机系统瘫痪的危险游戏最终被禁止了。1977年美国著名科普作家雷思在一本科幻小说中构思了一种能够自我复制的计算机程序。这种程序通过信息渠道传播控制了7000多台计算机的操作系统，造成了人类社会巨大的恐慌与动荡。1983年11月3日美国计算机安全专家Frederick Cohen在一次计算机安全学术讨论会首次提出计算机病毒的概念，并进行实验演示，证明了计算机病毒可以在短时间内对计算机系统造成严重破坏。历史往往存在着不幸的巧合，恰恰在5年以后的1988年11月3日，美国最大的计算机信息网络Internet遭到计算机病毒的攻击。病毒侵入网络中6200台小型机和工作站，造成近亿美元的直接经济损失。而这一事件的始作俑者不过是美国康乃尔大学的一名研究生。

从80年代末起，计算机病毒开始大规模泛滥，目前在全世界已经发现的计算机病毒有数千种之多。病毒不仅每年造成数十亿美元的经济损失，还扰乱人们的社会生活，例如1994年南非实现民族和解后第一次总统选举，就因为计算机系统遭病毒感染而推迟公布选举结果。

在80年代末和90年代初，编制计算机病毒多半是个人行为，一些掌握一定编程技术的人，其中不乏高级技术人员，出于个人目的，比如显示个人技巧、不适当地保护个人知识产权以及进行报复等而编制和扩散计算机病毒。值得注意的是在现代军事领域"软杀伤"的地位越来越突出，所谓软杀伤是指利用电子战等手段干扰破坏敌方的指挥武器系统，达到不战而屈敌之兵的目的。而计算机病毒则被当做是电子战的重要"武器"。据报导有的国家早已开始研究计算机病毒在军事领域

的应用，这无疑将促进“计算机病毒学”的进一步发展。军用病毒在战时将被用来攻击敌方的通讯线路和控制系统，传递有意错报信息，改变对方的通讯卫星软件，通过无线电通信系统侵入敌方的计算机指挥网络等等。毫无疑问在未来的战场上计算机病毒将成为令人生畏的“软”武器，但同时有关专家指出与传统硬武器比较，“军用病毒”技术更容易扩散到民间，对一般计算机用户造成危害。

计算机病毒于 1989 年传入我国，根据较严格的统计，到 1995 年上半年在我国已发现的病毒有 200 余种，其中有一部分出自本土病毒编制者。为了保护国家信息系统的安全，我国政府于 1994 年 2 月 18 日颁布了《中华人民共和国计算机信息系统安全条例》，其中明确规定“故意输入计算机病毒以及其他有害数据危害计算机信息安全”是违法行为。每一位用户都该加强计算机安全意识，保护自己的微机免受计算机病毒侵害，不传播计算机病毒，更不去制造病毒。

1.2 计算机病毒的分类

从 80 年代末至今不到 10 年时间，计算机病毒已经拥有一个很大的家族。让我们从不同角度，观察一下病毒家族中的各类病毒。

一、按破坏性质分类——恶性病毒与良性病毒

计算机病毒的编制者有意在病毒中插入具有破坏性的程序，如删除文件、向硬盘写入垃圾数据、格式化硬盘、封锁计算机的某些功能等等。这些病毒具有明显的破坏意图和行为，被称为恶性病毒。如 DISK KILLER 磁盘杀手、3．6 米凯朗基罗、JERUSALEM 耶路撒冷、PRGKILL PRG 文件杀手、888、DIEHARD 死硬、1091 和 1099 小时、Casper、幽灵等都是著名的恶性病毒。

与恶性病毒相对应，另有些病毒看上去似乎只是传染表现自己，并不主动破坏系统，如 BUPT、基因 GENE 等。BIRTHDAY 病毒表现时甚至还在屏幕上显示一段生日贺语，并无其它明显的破坏作用，称为良性病

毒。良性病毒是计算机病毒产生初期的一种说法，实际上任何病毒都有占用系统资源，干扰运行等不良影响，所以良性病毒的说法现在已经基本不用了。

二、按寄生部位分类——引导型病毒与文件型病毒

磁盘上的病毒不能独立公开地存在，否则用户明知是病毒就绝不会运行使用它。计算机病毒就象寄生虫一样，总是偷偷摸摸地侵占磁盘的某些部位，非法寄生在那里。当然病毒的寄生部位是有选择的，它们总是寻找可能被执行到的地方，就是磁盘的引导扇区或可执行文件，分别称为引导型病毒和文件型病毒，以及两者的组合——混合型病毒。有病毒寄生的磁盘引导区或可执行文件称为病毒的宿主。

病毒占据寄生部位是通过传染实现的，寄生部位和传染对象是一回事。

三、按传染方式分类——覆盖型与非覆盖型病毒

病毒在向寄生部位传染的时候总要占据一定磁盘空间。引导型病毒传染软盘一般多占一个扇区，混合型病毒传染硬盘引导区的同时要占用多个扇区。病毒究竟侵占哪些扇区往往是病毒编制者想当然决定的，所侵占扇区原来的数据全部被覆盖掉。当用反病毒工具处理覆盖型病毒的时候，只能清除病毒，无法恢复被病毒覆盖的数据。

文件型病毒传染的时候利用 DOS 的文件管理机制，能自动在磁盘上搜索尚未使用的部位写入病毒，一般不破坏磁盘数据。

四、按活动形态分类——磁盘静态病毒与内存动态病毒

病毒与其它软件一样是常驻磁盘的，称为磁盘病毒或“静态病毒”。通常所说的杀病毒就是指消除磁盘病毒。磁盘病毒随宿主进入计算机内存，非法参与计算机系统运行，进行传染破坏活动，处于活动状态，称为内存病毒或“动态病毒”，防病毒卡就是通过监视内存中动态病毒的活动而报警的。关掉计算机电源就可以中止内存病毒的当前活动，但

如果不消除磁盘病毒，下次开机病毒还会再次进入内存，所以只有杀除磁盘上的静态病毒才能彻底解除病毒危害。

五、按操作系统分类

已发现的计算机病毒大多是基于 DOS 系统的病毒，所谓 DOS 病毒是指病毒主要利用 DOS 操作系统的功能而且在 DOS 状态下就能传染破坏。DOS 病毒可以在网络上传播从而对网络造成严重的破坏。Windows 3.X 是基于 DOS 的操作系统，DOS 病毒仍会传染在 Windows 环境下运行的 DOS 文件，但不传染 Windows 可执行文件。1995 年 8 月脱离 DOS 的 Windows 95 终于出台，欧美国家立即报导发现攻击 Windows 95 的病毒，尽管这些报道的真实性还有待证实，但可以肯定在冯·诺依曼体系计算机中不管操作系统如何变化，都可能出现新的计算机病毒。

1.3 计算机病毒的结构

现代计算机软件，不论是专业公司的商品化产品，还是用户自行设计的应用程序，都采用模块化结构。计算机病毒作为一种特殊软件也不例外。一般来说，计算机病毒可以按其内部代码的功能划分成解密模块、安装模块、传染模块、破坏模块和表现模块。

一、解密模块

人类对信息进行加密保护已经有很悠久的历史了，在现代计算机中加密技术更是被广泛应用，很多软件都是加密出售的。早期的计算机病毒往往是不加密的明码病毒，容易被发现分析，不利于病毒的隐蔽传染，所以后来很多水平较高的病毒都进行了加密处理。正如密码电报必须经过解密翻译才能看懂一样，磁盘上的密码病毒读入内存后如果不进行解密，CPU 是不能识别执行的，所以加密病毒必然有一个解密模块。病毒随宿主进入内存后首先执行解密模块对病毒的密码部分进行解密，把密码还原成 CPU 能够直接识别的指令数据。解密模块是

病毒进入内存后 CPU 首先执行的程序，它本身当然不能加密，也就是说磁盘上的加密病毒由两部分组成：一部分是经过加密处理的密码部分，另一部分则是未加密的明码。明码部分的作用是对密码部分进行解密，即解密模块。

二、安装模块

磁盘上的计算机病毒随宿主进入微机内存后就立即在内存中安装自己。

1.占据内存

计算机病毒在占据内存的时候要做两件事，一是找一个合适的地方待下来，二是使占据"合法"化。

磁盘上的计算机病毒被读入内存时所占据的内存地址并不一定是病毒可以正常工作的地址。比如引导型病毒按照微机固有的开机流程中被读到内存 0000：7C00 地址，这个地址还将被随后读入的其它软件使用，病毒如果赖在这个地址不走就会被后续软件冲掉，所以引导型病毒将把自己迁移到内存中一个它认为合适的地方安营扎寨，通常是基本内高端。

病毒仅仅占据一块内存并不安全，还必须设法使别的软件不再使用它所占的内存，也就是使占据"合法"化。占据内存高端的引导型病毒通常修改基本内存容量值，该值是在微机开机时检测出来的，存放在内存 0000：0413 字单元，通常是 16 进制数 280，10 进制数为 640，即 640K 基本内存。病毒根据自己的需要减小该单元值。比如 NATAS 病毒把该值减去 6 成为 634，DOS 操作系统就会认为微机只有 634K 内存，从而不再使用病毒占据的高 6K 内存。这样用户白白丢失了 6K 内存，而病毒则有了避风港。

2.修改操作系统

微机的操作系统是开放的，用户可以修改扩充操作系统在微机上实现新的功能。修改操作系统的主要方式之一是扩充中断功能，中断的概念比较复杂，但并不神密。微机中断指令是 INT XX，其中 XX 为中

断号，可以把微机的软中断当作子程序来理解，CPU 执行 INT XX 指令就是调用 XX 号子程序。微机提供很多中断，合理合法地修改中断会给微机增加非常有用的新功能，比如 INT 10 是屏幕显示中断，原只能显示西文，而在各种汉字系统中都可以通过修改 INT 10 使微机能够显示中文。在另一方面，计算机病毒则篡改中断为其达到传染、激发等目的服务，与病毒有关的主要中断有：

INT 08 和 INT 1C 定时中断，每秒调用 18.2 次，有些病毒利用它们计时判断激发条件。

INT 09 键盘输入，病毒用于监视用户击键情况。

INT 10 屏幕输入输出中断，一些病毒用于在屏幕上显示字符图形表现自己。

INT 13 磁盘输入输出中断，引导型病毒用于传染病毒和格式化磁道。

INT 21 DOS 功能调用，包含了 DOS 的大部分功能，已发现的绝大多数文件型病毒修改 INT 21 中断，因此也成为防病毒卡的重点监视部位。

INT 24 DOS 的严重错误处理中断，文件型病毒常进行修改，以防止传染写保护磁盘时被发现。

中断子程序的入口地址存放在微机内存的最低端，病毒窃取和修改中断的入口地址获得中断的控制权，在中断过程插入病毒的“私货”。

3.在安装阶段除占据内存和修改操作系统外，大多数引导型病毒传染硬盘引导区；一些文件型病毒传染重要的 COMMAND.COM 文件；有的恶性病毒判断系统日期等条件，如与病毒预先设定的条件相符就立即激发。

三、传染模块

传染模块通过计算机病毒的安装而进驻内存，伺机搜寻传染目标。引导型病毒多监视 INT 13 的读写软盘过程，并利用 INT 13 的写过程把病毒写到软盘上。文件型病毒多监视 INT 21 的加载文件或列目录过

程，并利用 INT 21 提供的一组文件处理功能传染可执行文件。病毒传染模块的基本机理是：

1.监视微机运行状态，寻找传染对象和时机。病毒传染的对象是磁盘引导区和可执行文件，通常病毒选择用户读写磁盘的时候进行传染，因为这时磁盘驱动器灯要发亮，病毒混水摸鱼，借机把自己写到磁盘上，用户不容易发现。

2.分析将要传染的对象是否有病毒标志，如果有标志说明对象已经染上病毒，不需要再传染。

3.如果要传染的对象没有病毒标志，病毒就非法进行传染。

四、破坏模块

破坏模块是恶性病毒的直接表现，通常由激发条件和破坏程序两部分构成。病毒激发条件的设置是五花八门的。日期是病毒常用的条件，新闻媒体报刊资料中经常介绍某种病毒于某月某日激发，给人们留下深刻的印象。但日期并不是激发条件的唯一选择，有的病毒根据用户击键情况激发，又有的按微机染毒后的开机次数激发等。这些病毒的激发时机很难事先掌握，所以病毒激发是"突然"的，给人以猝不及防的感觉，较之按日期激发的病毒更为危险。

计算机病毒的破坏目标十分广泛：磁盘引导区、文件分配表、文件目录区、COM、EXE、OVL、ASM、PRG、BIN、C 等各种重要文件都成为计算机病毒的篡改删除对象。封锁打印机和键盘、干扰屏幕显示、强行演奏音乐、死机等也是病毒常用的伎俩。

五、表现模块

一些病毒具有强烈的表现欲，病毒表现时的现象比较明显，会给用户造成深刻的印象，所以往往根据表现症状来命名病毒：

毛毛虫病毒，表现为一条毛毛虫在屏幕上自左向右爬行，"吃"掉屏幕上的字符。

红心病毒激发时在屏幕上显示一连串红心，同时格式化硬盘。

火炬病毒激发时在屏幕上显示5支燃烧的火炬，同时用垃圾数据覆盖硬盘主引导区。

小球病毒激发时表现为一只小球在屏幕上跳动，微机进入死机状态。

扬基病毒和DABI病毒定时演奏音乐。

特别请注意病毒的表现和破坏往往同时发生，所以千万不要因为好奇而试图让病毒表现一下看看，更不能以病毒的"表现"当作判断病毒的依据，否则当看到病毒"画面"时，硬盘很可能已被破坏。

六、计算机病毒的标志

由于技术原因和病毒本身隐藏的需要，计算机病毒都采用特殊标志来防止重复传染同一对象。标志有两种：静态标志和动态标志。

引导型病毒和文件型病毒都有静态感染标志，往往是病毒内部的一组代码或字符。病毒在传染的时候先读出磁盘上的待传染对象，取特定位置上的代码与病毒标志相比较，如果两者相等说明已经染毒，不需要再次传染；如果两者不等就进行传染。有些文件型病毒利用文件目录表设置传染标志，病毒在传染文件的时候把目录中的时间、日期设成某一特殊值，以后再检测到这个特殊值就知道文件已经染毒了。病毒这种随意改变目录的行为往往造成文件管理上的混乱，是病毒的劣迹之一。

动态标志是检测内存中有无病毒活动的标记。当微机硬盘感染文件型病毒时，用户在一次上机过程中可能运行多个带毒软件。开机后运行第一个带毒文件的时候，病毒把自己安装到内存中成为动态病毒，同时也设立了动态病毒标志。而后再运行其它带毒文件时，文件病毒根据动态标志检测到内存中已经有病毒在活动就不再重复安装自己。引导型病毒是开机后读出的第一个磁盘扇区，而且每次开机只加载安装一次，所以不需要做动态判断。

1.4　计算机病毒的危害

在计算机病毒出现的初期，说到计算机病毒的危害，往往注重于病毒对信息系统的直接破坏作用，比如格式化硬盘、删除文件数据等，并以此来区分恶性病毒和良性病毒。其实这些只是病毒劣迹的一部分，随着计算机应用的发展，人们深刻地认识到凡是病毒都可能对计算机信息网络系统造成严重的破坏。计算机病毒主要危害有：

一、病毒激发对计算机数据信息的直接破坏作用

大部分病毒在激发的时候直接破坏计算机的重要信息数据，所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无意义的"垃圾"数据改写文件、破坏 CMOS 设置等等。一些典型的例子有：

DISK KILLER 磁盘杀手病毒，内含计数器，计数机制比较复杂，但大致可以估算出在硬盘染毒后累计开机时间 48 小时内激发，激发的时候屏幕上显示"Warning!! Don't turn off power or remove diskette while Disk Killer is Processing!"（警告！ DISK KILLER 正在工作，不要关闭电源或取出磁盘），改写硬盘全部数据。被 DISK KILLER 破坏的硬盘可以用专用软件修复，不要轻易放弃。

3.6 米开朗基罗病毒，一个破坏性极强却容易规避的病毒。3 月 6 日激发，把从内存 5000:5000 起的一堆无意义数据写到软盘或硬盘。修改微机日期或者 3 月 6 日不开机能躲避米氏病毒的激发。米开朗基罗是意大利著名画家，与计算机病毒本无任何瓜葛，只是由于画家的生日也是 3 月 6 日，才铸成了计算机病毒命名史上最大的冤案。

JERUSALEM 耶路撒冷病毒，即几乎家喻户晓的黑色星期五病毒，在西方人认为不吉利的 13 日又赶上星期五激发，删除当天运行的全部可执行文件。1989 年 11 月 13 日正赶上星期五，全世界有数十万台微机病毒激发，造成难以估量的损失。其它如 2128、新世纪病毒的破坏

作用也是删除文件,用户如果发现一个运行的文件被删除最好停机,不要再拿其他文件去"送死"。

PRGKILL PRG 文件杀手病毒每月 1 日删除各种数据库中的扩展名为 PRG 的程序文件。

888 病毒删除用 C 语言编制的扩展名为 C 的源程序文件和备份文件 BAK。

DIEHARD 死硬病毒删除汇编语言源程序文件 ASM 和 PASCAL 源程序文件 PAL。

1091 和 1099 小时病毒,用户一小时不击键激发;Casper 病毒 4 月 1 日激发;DDU 病毒开机 256 次激发。这几个病毒激发的时候都格式化硬盘或软盘。

幽灵病毒每次开机加密两个硬盘柱面,使微机依赖于病毒才能工作。

二、占用磁盘空间和对信息的破坏

寄生在磁盘上的病毒总要非法占用一部分磁盘空间。引导型病毒的一般侵占方式是由病毒本身占据磁盘引导扇区,而把原来的引导区转移到其它扇区,也就是引导型病毒要覆盖一个磁盘扇区。被覆盖的扇区数据永久性丢失,无法恢复。著名的大麻病毒在传染软盘的时候把原引导区转移到软盘的 1 面 0 道 3 扇区。对于 360KB 低密盘,1 面 0 道 3 扇区是根目录的最后一个扇区,如果软盘根目录下的文件不超过 96 个,看不出明显的破坏现象。但是对于 1.2MB 的高密盘,1 面 0 道 3 扇区是根目录的第三个扇区,一个目录扇区记录 16 个文件目录,所以高密盘的文件数(包括子目录)超过 32 个时,目录项就会丢失,可见大麻病毒对高密软盘的破坏是很严重的。感染了引导型病毒的磁盘在杀毒时通常只能恢复正确的引导区,而被病毒侵占的磁区是不可恢复的。

文件型病毒利用一些 DOS 功能进行传染,这些 DOS 功能能够检测出磁盘的未用空间,把病毒的传染部分写到磁盘的未用部位去。所以在传染过程中一般不破坏磁盘上的原有数据,但非法侵占了磁盘空间。

些文件型病毒传染速度很快，在短时间内感染大量文件，每个文件都不同程度地加长了，就造成磁盘空间的严重浪费。特别是黑色星期五和变种 FLIP 这两个病毒，它们对同一个文件重复感染，使文件不断加长，所以黑色星期五有个别名叫做疯狂拷贝病毒。曾发现一个 NOVELL 网络中原长度不到 3KB 的 COM 文件被变种 FLIP 病毒传染后长度增加到近 64KB，是原文件长的 20 多倍，这个网络系统很快就崩溃了。

三、抢占系统资源

除 VIENNA、CASPER 等少数病毒外，其它大多数病毒在动态下都是常驻内存的，这就必然强占一部分系统资源。病毒所占用的基本内存长度大致与病毒本身长度相当，如果病毒开劈一个缓充区则还要长一些。幽灵、秋水、NATAS 等混合型病毒可能占用 4～10KB 内存。各种应用软件对内存的要求越来越高，微机并不富裕的内存反而被病毒占去一部分就更显得紧张，会造成一部分软件不能运行。除占用内存外病毒还抢占中断接口，干扰系统运行。微机操作系统的很多功能是通过中断调用技术来实现的。病毒为了传染激发，总是修改一些有关的中断地址，在正常中断过程中加入病毒的“私货”，从而干扰了系统的正常运行。

四、影响微机速度

病毒进驻内存后不但干扰系统运行，还影响微机速度，主要表现在：

1.病毒为判断传染激发条件，总要对微机的工作状态进行监视，这相对于微机的正常运行状态既多余又有害。很多病毒利用 INT 8 或者 INT 1C 中断计算时间，这两个中断每秒钟发生 50 次，也就是微机运行过程中每一秒都会有 50 次进入病毒程序中去兜圈子，白白占用了 CPU 时间。

2.有些病毒为了保护自己，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态，CPU 每次寻址到病毒处时要先

运行一段解密程序把加密的病毒解密成合法的 CPU 指令再执行；而病毒运行结束时再用一段程序对病毒重新加密。这种所谓动态加密的病毒每执行一次都要解密和加密各一次，为此 CPU 要额外执行数千以至上万条指令，可以看出病毒为了达到自己的目的是无所不用其极的。

3.病毒在进行传染时同样要插入非法的额外操作，特别是传染软盘时不但微机速度明显变慢，而且软盘正常的读写顺序被打乱，发出刺耳的噪声。

五、计算机病毒错误与不可预见危害

计算机病毒与其它计算机软件的一个很大差别是病毒的无责任性。编制一个完善的计算机软件需要耗费大量的人力、物力，经过长时间调试完善，软件才能推出。但在病毒编制者看来既没有必要这样做，也不可能这样做。很多计算机病毒都是个别人在一台计算机上匆匆编制调试后就向外抛出。反病毒专家在分析大量病毒后发现绝大部分病毒都存在不同程度的错误，有些错误甚至以讹传讹长期存在。比如 DOS 系统中可执行文件的扩展名 COM 和 EXE 只是一个外部表象，在 DOS 加载执行文件的时候不是根据扩展名，而是根据文件的内部标志来决定文件的类型。但是绝大多数文件型病毒都只根据扩展名判断可执行文件的类型进行传染，由此造成的死机想象屡见不鲜，可以说在上千种病毒中能正确判断文件类型的病毒不多。

错误病毒的另一个主要来源是变种病毒。有些初学计算机者尚不具备独立编制软件的能力，出于好奇或其它原因修改别人的病毒。比如 FLIP 病毒的，原型并不重复感染，但修改者没有搞清楚病毒的全部机理就改动了病毒成为新变种。变种 FLIP 重复传染 COM 和 EXE 文件，其破坏性比著名的黑色星期五还要恶劣。

计算机病毒错误所产生的后果往往是不可预测的，反病毒工作者曾经详细指出黑色行期五病毒存在着 9 处错误，乒乓病毒有 5 处错误等等。但是人们不可能花费大量时间去分析数千种病毒的错误所在。大量含有未知错误的病毒扩散传播，其后果是难以预料的。

六、计算机病毒的兼容性对系统运行的影响

兼容性是计算机软件的一项重要指标，兼容性好的软件可以在各种微机环境下运行；反之兼容性差的软件则对运行条件"挑肥拣瘦"，要求机型，要求操作系统版本等，如果商品软件的兼容性差其销路一定不好。要提高软件兼容性除了正确的理论设计外，更重要的是要在各种环境下对软件进行实测，既要在不同型号的 CPU 机器上运行，又要通过各种支持平台测试。而病毒的编制者一般不会做这些工作，即使一些"高手"编制的病毒也存在着兼容性问题。比如著名的 DIR-II 和 DONG 病毒，据认为它们的编程技术都很高，但由于他们依赖于 DOS 3 系统，所以带有这些病毒的文件在高版本 DOS 下运行时将造成死机现象。更为恶劣的 2803 病毒在 DOS 3 下尚能工作，但在 DOS 6 环境下传染时磁盘驱动器发出极难听的声音，并且严重损坏磁盘。又比如在硬件兼容方面，乒乓病毒中用了一条强行修改 CPU 指令段地址寄存器的指令 MOV CS, AX，这在最早期的 8088、8086 微机中是允许的，但在 80286 以上微机上都被认为是非法指令造成死机。

七、计算机病毒给用户造成严重的心理压力

据有关计算机销售部门统计，微机售出后用户因怀疑"计算机有病毒"而提出咨询约占售后服务工作量的 60% 以上。经检测确实存在病毒的约占七成，另有三成情况只是用户怀疑，而实际上微机并没有病毒。那么用户怀疑病毒的理由是什么呢？多半是出现诸如微机死机、软件运行异常等现象。这些现象确实很有可能是计算机病毒造成的，但又不全是。实际上在微机工作"异常"的时候很难要求一位普通用户去准确判断是否是病毒所为。大多数用户对病毒采取宁可信其有的态度，这对于保护微机安全无疑是十分必要的，然而往往要付出时间、金钱等方面的代价。仅仅怀疑病毒而冒然格式化磁盘所带来的损失更是难以弥补。不仅是个人单机用户，在一些大型网络系统中也难免为甄别病毒而停机。总之计算机病毒象"幽灵"一样笼罩在广大计算机用户

心头，给人们造成巨大的心理压力，极大地影响了现代计算机的使用效率，由此带来的无形损失是难以估量的。

1.5 深刻认识计算机病毒的传染性

准确描述计算机病毒的特性并不是一件容易的事情，比方说可以罗列出计算机病毒有传染性、潜伏性、隐蔽性，给人的印象似乎是并列的三个特性。但实际上它们是相互关联的，而且后二者是为前者服务的。另外计算机病毒的破坏性也是众所周知的，要防止病毒的危害发生，就要深刻了解计算机病毒的传染性。

一、传染是计算机病毒最基本的特性

计算机病毒为什么要传染呢？道理很简单，就是计算机病毒的目的并不在于只破坏影响一台或少数计算机的运行，而是想影响而越宽越好，通过一传十，十传百的过程侵入为数众多的计算机系统。在计算机病毒出现的初期，一种并不复杂高明的病毒传播到世界各地，侵入上万以至几十万台微机的例子屡见不鲜。

传染性，也就是自我复制是计算机病毒最基本的特性，也是区分病毒和有害程序的标志。比如某银行职员编制了一个软件专用于通过银行计算机非法提金，这是一种计算机犯罪行为，他所编的那个软件当然是有害软件，但不是计算机病毒。另一方而通常所说的所谓良性病毒虽然似乎没有什么破坏性，但它们偷偷摸摸地进行自我复制，终归仍然是病毒。

关于病毒与非病毒区分还有一个有趣的例子。使用过 CPAV 反病毒软件的用户都知道 CPAV 有一项免疫功能，作用是给可执行文件加一层保护。免疫后的可执行文件长度要增加，增加的长度就是保护层的长度。无独有偶，94 年发现的 INOC 病毒具有相类似的特性。INOC 病毒本身长 1786 字节，如果一个感染 INOC 病毒的文件再染上别的病毒，INOC 病毒会把后染的病毒清掉。INOC 中有一段英文宣示了它的

"反病毒"作用：

Anti Virus

If your software has been inflected other viruses, run your software, then the virus will be cleaned!

大意是"如果你的软件感染了其它病毒，运行你的软件病毒就会清除！"。CPAV 的免疫功能和 INOC 作用类似，两者的归宿却截然相反。前者成为反病毒的明星，后者却被认定是病毒。其原因在于 CPAV 的免疫功能是根据用户的意愿，在用户本人控制下是实施的，而 INOC 却是背着用户非法传染到文件上的。

二、传染性、潜伏性、隐蔽性

计算机病毒侵入微机硬盘后一般并不立即激发，而是等待当微机状态符合病毒预先设定的激发条件时才激发，从病毒入侵微机到病毒激发这段时间就是病毒的潜伏期。病毒之所以藏而不发正是为了在潜伏期内广泛地传染，所以病毒的潜伏期就是病毒的传染期。

在传染期内病毒将尽量隐蔽自己不被用户发现。磁盘静态病毒多采用加密技术，甚至产生了变形病毒；内存动态病毒则采用变化的手段修改中断、占用内存，尽量逃避反病毒软件的侦测，病毒隐蔽的目的是为了其自身顺利地传染。

三、传染性与破坏性

就一台微机而言，病毒的危害程度主要取决于病毒破坏的目标和破坏的深度。而对整个社会而言，计算机病毒的危害显然与其传播的广泛程度紧密相关。一个传染性强的病毒有可能给社会造成更大的危害。

四、病毒传染性与反病毒的关系

如前所述计算机病毒传染是为了危害更多的微机。但在另一方面也正是病毒的传染性提供了发现和消除病毒的时机。

计算机病毒传染的基本条件是尽可能不被用户发现，使微机染上病毒后仍能运行，由此可以得出重要的结论：

> 在病毒激发之前，感染病毒微机的绝大部分磁盘资源没有遭到破坏。

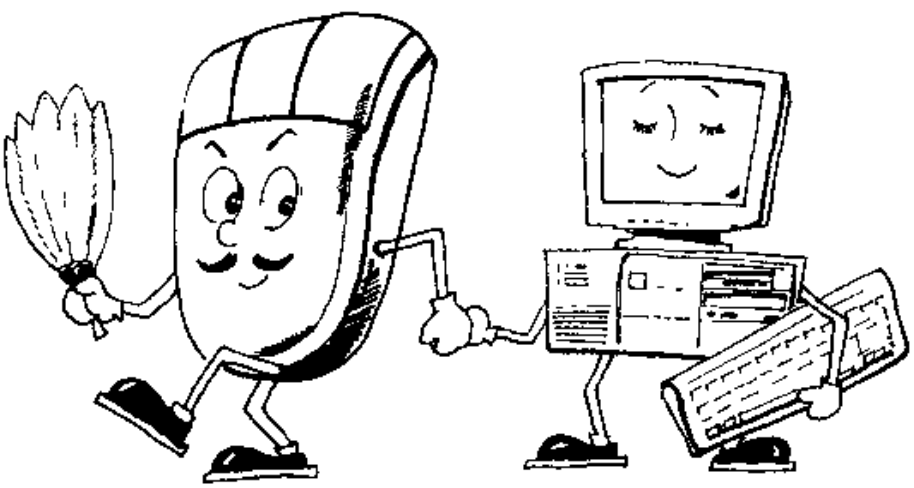
微机感染了引导型病毒，但仍能上电开机说明微机引导所要求的重要数据信息仍然存在，只要用正确的引导程序去替代占据磁盘引导区的病毒程序就杀除了病毒。

可执行文件感染了病毒，但仍能运行意味着文件本身未被破坏，往往只是多了一条病毒尾巴，只要去掉尾巴，修复少量代码数据就恢复了可执行文件的原状。

商品化通用消病毒工具都是针对病毒传染特性设计的，用户应正确把握杀病毒软件的使用时机，消除传染阶段的病毒，保护自己的微机资源。

第二章

磁盘结构与引导型病毒



2.1 磁盘结构

磁盘是微机的外存储设备，包括软盘和硬盘，它们都是计算机病毒的寄生地和攻击目标。

一、软磁盘

大家知道，磁盘必须格式化后才可使用，在格式化的时候把磁盘表面划分成磁道和磁区。磁道是由外向里分布的一组同心圆，最外面的是 0 道。在每一磁道中又划分成若干扇形磁区，每个扇区可以存储 512 字节，每一字节是一个 8 位 2 进制数。目前常用软盘磁道和扇区的划分情况如下：

双面双密度 5 英寸盘，40 条磁道，每道 9 扇区，容量 360KB。

双面高密度 5 英寸盘，80 条磁道，每道 15 扇区，容量 1.2MB。

双面双密度 3 英寸盘，80 条磁道，每道 9 扇区，容量 720KB。

双面高密度 3 英寸盘，80 条磁道，每道 18 扇区，容量 1.44MB。

软盘的面、磁道和扇区都有固定的编号。以 5 英寸高密盘为例，面的编号是 0 和 1，对应为软盘驱动器的磁头 0 和 1；磁道编号为 0 到 79 共 80 道；扇区编号为 1 到 15。共有 2(面) X 80(道/面) X 15(扇区/道) = 2400 个扇区，每个扇区有 512 字节，即 0.5KB，全盘共 1200KB，就是通常所说的 1.2MB 软盘。

为了对磁盘进行管理，一些扇区被赋予专门的用途，这些扇区常成为计算机病毒传染或攻击的对象，这些扇区是：

DOS 引导扇区，对于各种软盘 DOS 引导扇区都位于 0 面 0 道 1 扇区。引导扇区由两部分构成：引导程序和磁盘参数表。引导扇区是用 FORMAT 命令格式化过程中产生的。各种引导型病毒都是用一段病毒程序插在引导程序之前运行，完成病毒的初始化。

文件分配表，英文缩写是 FAT。为方便有效地管理文件，DOS 以簇为单位来读写文件，一簇由若干扇区组成，磁盘上有顺序编号的若干

簇。FAT 记录了文件在磁盘上的簇号分布情况，DOS 在读写磁盘文件的时候首先从目录表中获得文件的起始簇号，然后再根据 FAT 中的簇链式结构信息读取整个文件。由于 FAT 十分重要，所以磁盘都建立了两个 FAT，分别称为 FAT1 和 FAT2，FAT2 是 FAT1 的备份。不同容量的磁盘 FAT 的大小，也就是所占的扇区数是不同的，显然磁盘容量越大，FAT 表就越长。5 英寸高密盘每个 FAT 表占 7 个扇区，即 FAT1 位于 0 面 0 道的 2 到 8 扇区；FAT2 从 0 面 0 道的 9 扇区到 15 扇区。由于 FAT 的特殊结构它可能成为计算机病毒攻击的目标。

根目录表顾名思义记录着磁盘的有关目录项，根目录表紧接在 FAT2 后面，对于 5 英寸高密盘，DOS 引导区和两个 FAT 恰好占用了 0 面 0 道的 15 个扇区，那么根目录表是在 0 面 1 道还是 1 面 0 道呢？为了减少磁头的移动次数，磁头在访问 0 面 0 道后换面不换道，即紧接着访问 1 面 0 道，所以 5 英寸高密盘根目录表从 1 面 0 道 1 扇区开始到 1 面 0 道 14 扇区，长度为 14 个扇区，每扇区可存 16 个文件的目录。

目录表与计算机病毒关联较多，有必要详细了解。下面是一片 5 英寸高密系统盘根目录表开始的部分内容，请注意左边的数字是 16 进制数。

```
49 42 4D 42 49 4F 20 20-43 4F 4D 27 00 00 00 00    IBMBIO  COM'....
00 00 00 00 00 00 00 60-43 11 02 00 27 5C 00 00    .......`C...'.
49 42 4D 44 4F 53 20 20-43 4F 4D 27 00 00 00 00    IBMDOS  COM'....
00 00 00 00 00 00 00 60-43 11 31 00 B8 77 00 00    .......`C.1..w..
43 4F 4D 4D 41 4E 44 20-43 4F 4D 20 00 00 00 00    COMMAND COM ....
00 00 00 00 00 00 00 60-43 11 6D 00 F4 62 00 00    .......`C.m..b..
34 32 30 31 20 20 20 20-43 50 49 20 00 00 00 00    4201    CPI ....
00 00 00 00 00 00 00 60-9F 0F 9F 00 C1 42 00 00    .......`.....B..
```

每个目录项用 32 个字节表示，其意义分别是：

第 1 到 8 字节，用 ASCII 码表示的主文件名，如 IBMBIO。

第 9 到 11 字节，用 ASCII 码表示的扩展文件名，如 COM。

第 12 字节，文件的属性，用于表征文件含义和读写权限。当一个

文件具有只读属性时，该文件不能直接被改写，所以有的文章中介绍用置只读属性的方法来防止文件被病毒传染。实际上这种作法的保护作用十分有限，因为大量文件型病毒在传染时都先用 AH = 43 的 INT 21 调用修改文件属性为一般读写文件再进行传染。DOS 6 系统在格式化时已经置 COMMAND.COM 文件为只读属性，但大部分病毒都能传染 COMMAND.COM。属性还用于表示隐含文件，如上面目录中的前两个系统文件列目录时是看不到的。

第 13 到 22 字节备用。

第 23 和 24 字节，文件最后一次修写的时间。这是病毒经常篡改利用的一个数据，其 16 位 2 进制数记录方式是：

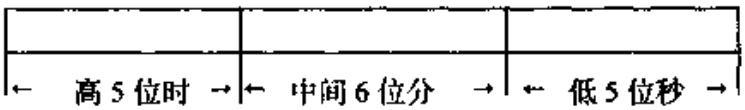


图 2-1 DOS 文件的时间记录

高 5 位 2 进值数存小时数，2 进制数域是 00000 到 11111，相对应的 10 进数域是 0 到 31，实际用 0 到 23 表示小时值，24 到 31 不用。

中间 6 位 2 进值数存分数，2 进制数域是 000000 到 111111，相对应的 10 进数域是 0 到 63，实际用 0 到 59 表示分值，60 到 63 不用。

低 5 位 2 进值数存秒数，2 进制数域是 00000 到 11111，相对应的 10 进数域是 0 到 31，但实际一分种有 60 秒，0 到 31 不足以表达全部秒值，所以低 5 位的每一计数代表 2 秒，即计数 0 代表 0 秒；1 代表 2 秒；2 代表 4 秒……。按照这种规定，低 5 位计数的 0 到 29 代表 0 秒到 58 秒，低 5 位的 30 和 31 两个值不用。

可以看出由于时间采用 60 进制，而计算机使用 2 进制，所以 DOS 的小时、分、秒计数中都有一些不用的数。在正常的 DOS 文件管理机制下不会产生这些计数，比如小时数不会是 30，但计算机病毒经常会强行修改时间计数。

第 25 和 26 字节，文件最后一次修改的日期。16 位 2 进制数记录

方式是：

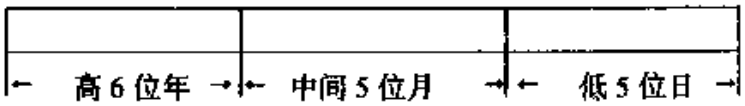


图 2-2　DOS 文件的日期记录

高 6 位 2 进制数存年度与 1980 年的差值，即用 1980 加上该计数值得到公元年度值。2 进制数域是 000000 到 111111，相对应的 10 进数域是 0 到 63，实际用 0 到 19 与 1980 相加表示 1980 年到 1999 年。

中间 5 位 2 进制数存月份，2 进制数域是 00000 到 11111，相对应的 10 进制数域是 0 到 31，实际用 0 到 11 表示 1 到 12 月。

低 5 位 2 进值数存日期，2 进制数域是 00000 到 11111，相对应的 10 进制数域是 0 到 31，实际用 0 到 30 表示 1 到 31 日。

第 27 和 28 字节，文件的首簇号。为方便有效地管理文件，DOS 以簇为单位来读写文件，一簇由若干个扇区组成。当 DOS 访问一个文件时首先根据目录表中的首簇号读取文件的第一簇，再根据 FAT 读取其它各簇。

首簇号也成了计算机病毒利用的对象。DIR-2 是一个很特殊的病毒，病毒本身占据磁盘的最后一簇，在它传染文件的时候并不修改被传染的文件，而是修改磁盘文件表中所有可执行文件的首簇号都指向磁盘的最后一簇，也就是指向病毒，而文件原来的首簇号则被加密后保存在备用的第 21 和 22 字节。执行文件表中任何一个文件都先读磁盘最后簇的 DIR-2 病毒，而且其传染速度极快。

第 29 到 32 字节是文件的长度。除少数特例外，可执行文件被病毒感染后长度都要增加。

软盘的 DOS 引导区、FAT 表、根目录表是在软盘格式化过程中形成的。软盘上的其它扇区都是数据区，用于记录存放各种文件。子目录被当做一种特殊文件来处理，其记录格式与根目录表是相同的。

二、硬磁盘

硬盘的速度快，容量大，是微机最重要的外存储设备。硬盘由同轴的多个盘片构成，目前市场上出售的硬盘以 4 片和 8 片盘的居多。每片盘有上下两个读写磁头，所以磁头数是盘片数的倍数，比如 8 片盘有 16 个磁头，编号从 0 到 15。与软盘一样硬盘在物理上也被划分成磁道和扇区来使用，各个盘片的同一磁道是同轴同半径的圆，从而形成了“柱”的概念。用头、柱、扇区来描述硬盘与用面、道、扇区来描述软盘是一致的。

硬盘的 0 头 0 柱 1 扇区是主引导扇区，由主引导程序和硬盘分区表两部分组成。在微机应用历史上，硬盘曾被设定最多可以分成 4 个区来使用，以装载不同的操作系统。DOS 的 FDISK 命令就是分区命令，分区的结果记录在分区表中。分区表位于硬盘主引导扇区尾部，从倒数第 66 个字节起，4 个分区记录各长 16 字节，总计 64 字节。4 个分区中有一个是活动分区，即微机上电引导的分区。主引导程序的作用是找到分区表中的活动分区，读出活动分区的第一个扇区，继续微机的自举引导。

绝大多数微机使用 DOS 操作系统，硬盘的活动分区是 DOS 分区，DOS 分区的第一个扇区与软盘一样是 DOS 引导区，一般位于 1 头 0 柱 1 扇区。在 DOS 分区中同样有两个 FAT 表和根目录表。

当由硬盘引导开机时，主引导区是微机开机后读出并执行的第一个扇区，而 DOS 引导区是读出并执行的第二个扇区，它们都是引导型病毒感染的对象，但病毒只传染其中一个。目前大多数引导型病毒侵占硬盘的主引导区，只有少量感染硬盘的 DOS 引导区。

2.2 微机引导过程

计算机病毒中的一大类，即引导型病毒与微机的上电引导过程紧密相关。微机引导指的是从打开微机电源到出现 DOS 提示符这一整

个过程，引导的最终结果是微机准备就绪，可以接受用户输入的各种DOS命令。已经上电的微机按下冷启动键RESET将重新引导，按热启动键Ctrl-Alt-Del也将重新引导，但与冷启动有一些差异，有些病毒利用热启动进行破坏，所以在处理病毒问题的时候要慎用热启动键。

微机的引导过程十分复杂，我们只讨论与病毒和反病毒有关的部分。当用户打开电源开关后经过电源复位，电源电压在极短的时间内达到微机的正常工作电压，中央处理器CPU立即就要读取和执行指令。CPU所读取和执行的第一批指令存放在微机内部的一块固态存储器上，通常是EPROM。EPROM与RAM的特性不同，通常所说的微机有兆内存指的是RAM容量，RAM中存储的数据在关闭微机电源后将"丢失"，下一次开机需重新存入。而EPROM是非易失性存储器，存储的指令数据与电源无关，因此微机一上电EPROM就能立即提供指令数据，支持CPU开始工作。微机主板上的EPROM又有一个专用名字叫BIOS ROM，BIOS是基本输入输出系统的意思，BIOS完成的主要工作有：

1.微机硬件系统的自检，包括对CPU、RAM、ROM、键盘、磁盘驱动器、DMA控制器、定时器、中断控制器、通讯接口等硬件设备的检测。如果在开机过程中蜂鸣器发出短促声音，屏幕上显示某某号错误，就是硬件自检没有通过的提示。根据自检错误的部位和程度分为"致命"错误和"非致命"错误，BIOS会做出不同的处理。

2.初始化基本I/O驱动程序和中断地址。

3.检测是否存在扩展ROM，如果存在则执行扩展ROM。各种反病毒卡可以在此时引导，优先于下面第4步可能进入微机内存的病毒。

4.读取磁盘的第一扇区到内存0000:7C00地址，接着从0000:7C00地址起读取和执行指令。

至此BIOS ROM的引导工作完成，但整个DOS引导过程没有结束，接下去的工作从内存0000:7C00地址继续。如果引导盘是合法的DOS系统软盘，第4步读出的是正确的DOS引导程序。从0000:7C00地址起DOS引导程序根据磁盘参数表计算出DOS系统第一个隐含文件

IBMBIO.COM(或 IO.SYS)在磁盘上的位置,把该文件读入内存,控制权交给 IBMBIO.COM,继续 DOS 的引导全过程,直到出现 DOS 提示符。硬盘的引导过程与软盘基本类似,但硬盘多了一个主引导区,所以在第 4 步首先读出主引导区,主引导程序根据分区表读出硬盘 DOS 引导区。

2.3 引导型病毒

上一节介绍了在正常引导过程中 BIOS ROM 引导的第 4 步把正确的 DOS 引导程序读到内存 0000:7C00 地址,并且从 0000:7C00 地址起继续引导开机的情况。现在提出这样一个问题,如果磁盘的第一个扇区不是正确的引导程序情况又会怎样?答案是不论在 BIOS ROM 引导第 4 步读出的是什么,CPU 都将从 0000:7C00 起执行指令。这就给了计算机病毒以可乘之机,所谓引导型病毒正是采用偷梁换柱的手法,由病毒本身占据磁盘的第一个扇区,而把原来引导扇区移到磁盘其它位置。这样在 BIOS ROM 引导的第 4 步首先读出并存入内存 0000:7C00 地址的第一个扇区是引导型病毒,接下去 CPU 将从 0000:7C00 起执行病毒程序。

一、引导型病毒的寄生方式

引导型病毒程序占据软盘的第一个扇区,软盘原来的引导扇区被移到磁盘的另一扇区,该扇区的数据被覆盖。早期的一些老病毒编制比较草率,往往选定固定的扇区存放原引导区。比如 AZUSA 病毒把原引导区存放在软盘 1 面 39 道 8 扇区,因为 39 转换成 16 进制数是 27,所以又叫 2708 病毒。1 面 39 道 8 扇区是 360K 软盘的最后一个扇区,影响较小,而对于 1.2M 和 1.44M 的高密软盘破坏作用较大。较新的病毒,如下面将介绍的 255 病毒则能根据软盘的尺寸容量计算出"合适"的扇区存放原引导区。EXEBUG 病毒编制得十分紧凑,病毒程序本身包括引导程序的功能,就不需要另占扇区。巴基斯坦、磁盘杀手等病

毒占用多个磁盘扇区，对软盘数据的破坏就更大些。

引导型病毒在硬盘上的寄生与软盘不太一样，多数病毒感染硬盘的主引导扇区。由于主引导扇区本来就有较多的空余字节，所以病毒往往只是插入空闲区，而不需要把原扇区移走。

二、引导型病毒在内存中的安装

在微机引导过程中首先读出病毒程序，病毒在内存中寻找合适的地方藏身，大多数病毒安装在基本内存高端。在 BIOS ROM 检测内存 RAM 的时候已经把基本内存 K 数存入 0000:0413 字单元，所有的新型微机都有 640K(16 进制 280) 基本内存，即 0000:0413 字元的值是 280，病毒可以直接获取该单元值，减去病毒所需内存 K 数后再存回去，也可以通过 INT 12 调用达到同样目的。而后病毒传送到内存高端。但高端基本内存并不是唯一选择，内存中有些小块内存 DOS 系统没有使用，计算机病毒无孔不入，把小块空闲内存作为自己的栖身之地，BASIC 病毒即是一例，任何内存检测软件都查不出这种利用空闲内存的病毒。

病毒在内存中找到栖身之地后，还要修改磁盘输入输出 INT13 中断，获取 INT13 的控制权，为开机后传染软盘作准备。最后读出原引导区，跳转到原引导程序继续运行。

三、引导型病毒的传染机理

微机软硬盘的配置和使用情况是不同的。软盘容量小，可以方便地移动交换使用，在微机运行过程中可能多次更换软盘；硬盘做为固定设备安装在微机内部使用，大多数微机配备一只硬盘。引导型病毒针对软硬盘的不同特点采用了不同的传染方式。

引导型病毒利用在开机引导时窃获的 INT13 控制权，在整个微机运行过程中随时监视软盘操作情况，趁读写软盘的时机读出软盘引导区，判断软盘是否染毒，如未感染就按病毒的寄生方式把原引导区写到软盘另一位置，把病毒写入软盘第一个扇区，从而完成对软盘的传染。

染毒的软盘在软件交流中又会传染其他微机。由于在每个读写阶段病毒都要读引导区，既影响微机工作效率，又容易因驱动器频繁寻道而造成物理损伤。

引导型病毒对硬盘的传染往往是在微机上第一次使用带毒软盘时进行的，其体步骤与软盘传染相似，也是读出引导区判断后写入病毒。

四、引导型病毒的破坏行为

引导型病毒的破坏行为与程度随病毒种类而异，多数发生在安装阶段。在安装阶段内存 DOS 系统尚未建立，病毒难于进行文件级操作，所以很多病毒直接攻击硬盘的重要磁道。

五、引导型病毒的其它特点

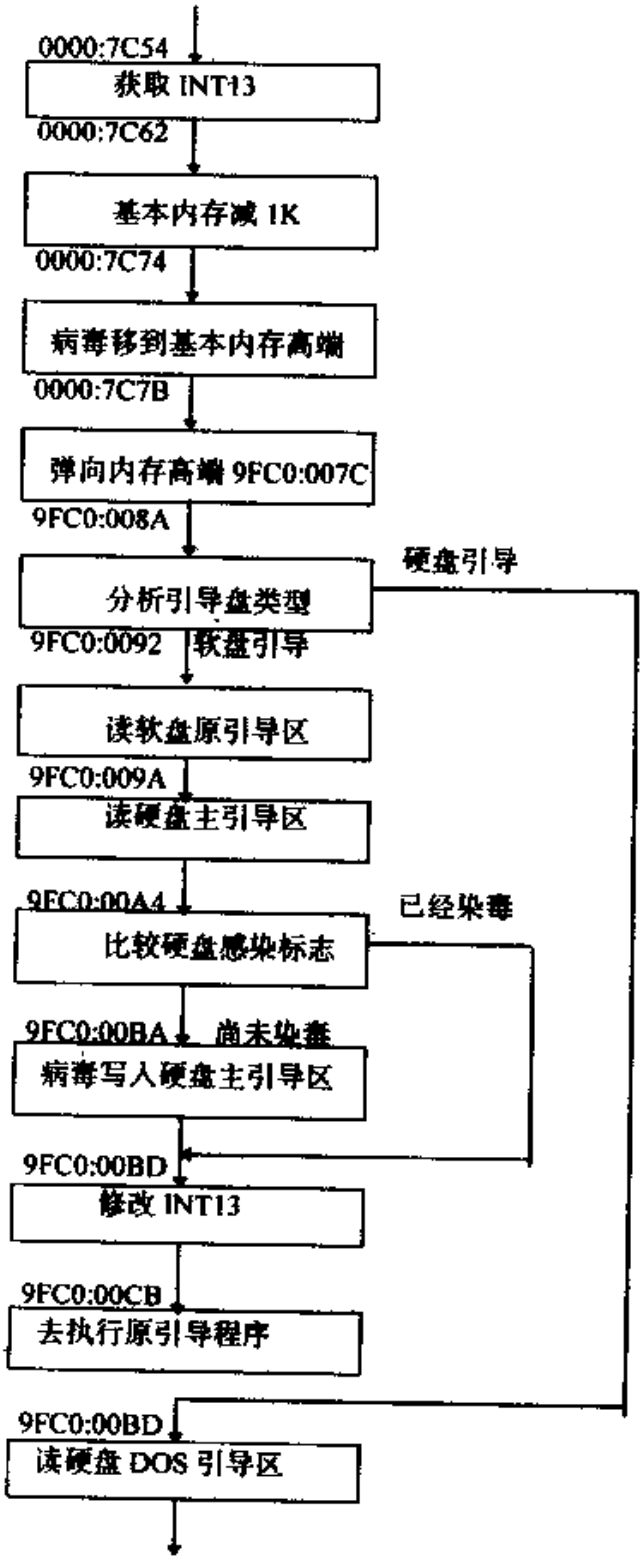
由于磁盘一个扇区的长度有限，为 512 字节，加上引导型病毒安装时微机内存中可利用的系统资源并不丰富，所以引导型病毒的结构一般比较简单，不同病毒之间大同小异，很少做加密处理。

2.4 255 恶性病毒分析

1995 年 9 月华东地区新发现一个破坏性很大的引导型病毒，当时国内外的杀毒软件尚不能杀除它。这个病毒内设计数器，在它感染微机硬盘后，微机每引导 1 次，包括上电开机和冷热启动，计数值加 1，当计数达 255 次病毒激发格式化硬盘 0 头 0 道，因此命名为 255 病毒。通过对 255 病毒的简要分析可以看出引导型病毒是如何强占内存、伺机传染和破坏的。

一、安装和破坏模块(见图 2-3)

二、传染模块(见图 2-4)


0000:7C54
获取 INT13
0000:7C62
基本内存减 1K
0000:7C74
病毒移到基本内存高端
0000:7C7B
弹向内存高端 9FC0:007C
9FC0:008A
分析引导盘类型
硬盘引导
9FC0:0092
软盘引导
读软盘原引导区
9FC0:009A
读硬盘主引导区
9FC0:00A4
比较硬盘感染标志
已经染毒
9FC0:00BA
尚未染毒
病毒写入硬盘主引导区
9FC0:00BD
修改 INT13
9FC0:00CB
去执行原引导程序
9FC0:00BD
读硬盘 DOS 引导区

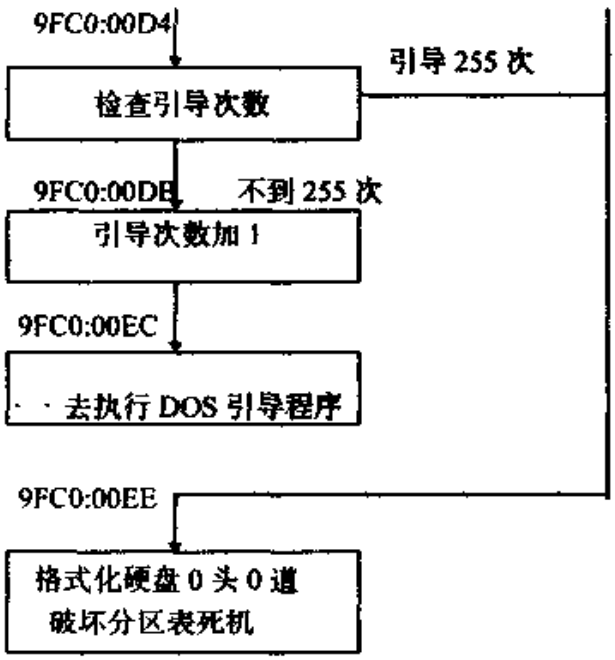


图 2-3　255 病毒的安装和破坏模块

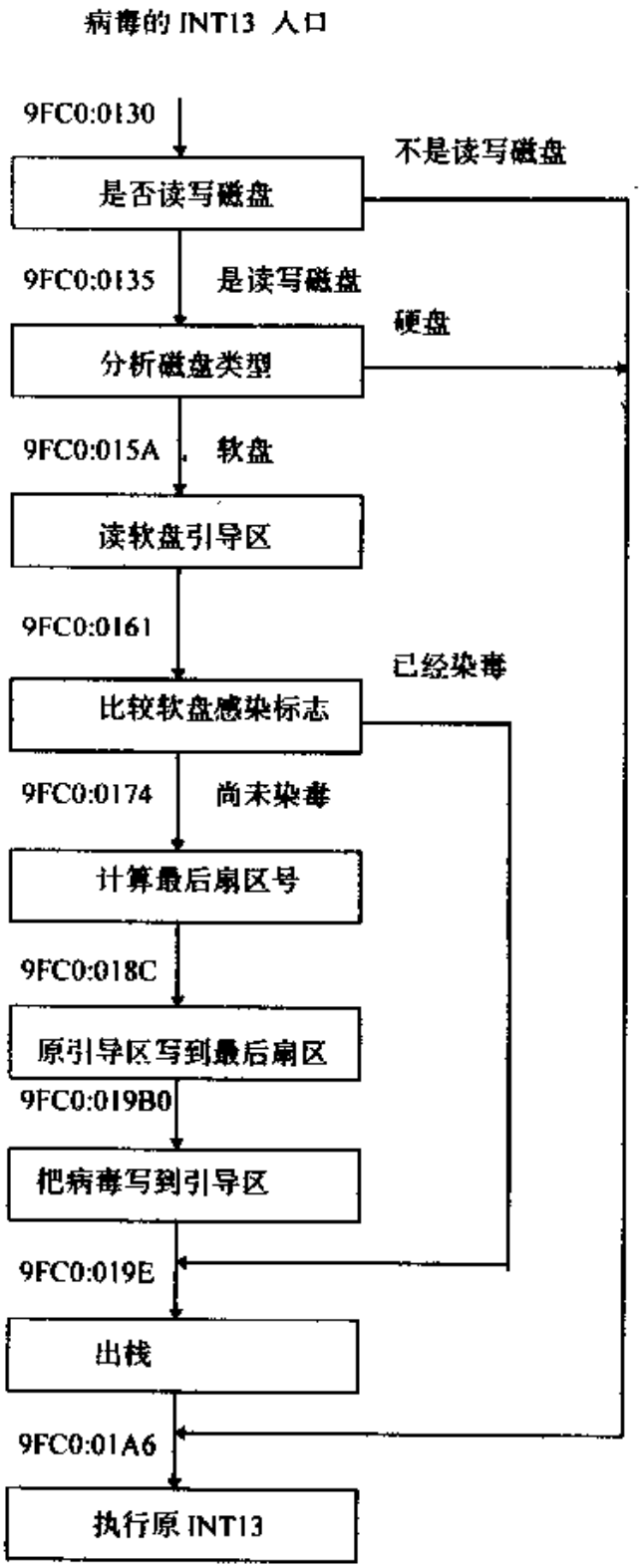
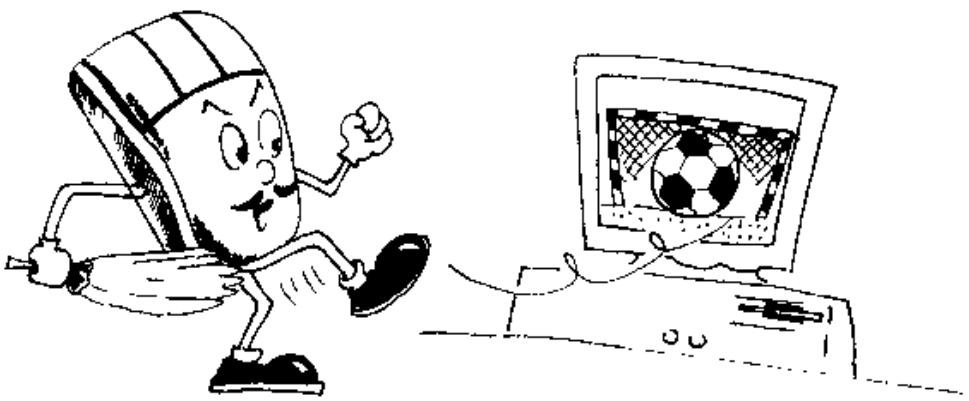


图 2-4　255 病毒的传染模块

第三章

可执行文件与文件型病毒



磁盘上的可执行文件主要指扩展名为 COM 和 EXE 的文件，简称 COM 文件和 EXE 文件。当用户通过键盘打入这些文件的主文件名回车后软件即可运行，完成既定的软件功能。比如打入字处理软件 WS.COM的主文件名 WS 回车进行文字处理；打入 PC 工具软件 PCTOOLS.EXE的主文件名 PCTOOLS 回车观察磁盘文件等。COM 和 EXE 文件是一系列机器语言指令的集合，机器语言指令是 CPU 唯一可以直接读取执行的指令，效率最高，速度最快。计算机病毒中的一大类，即文件型病毒就寄生在可执行文件上。

磁盘上的批处理 BAT 文件也可以通过命令方式执行，但 BAT 文件的实质是 DOS 内部命令和外部命令的顺序组合，目前还没有发现传染 BAT 文件的病毒。

3.1 COM 和 EXE 文件

一、可执行文件的加载与执行

当用户在 DOS 提示符下用键盘打入一组字符回车后，这组字符被当作一个命令看待。查找的顺序是先找 DOS 内部命令，再搜索 DOS 外部命令，即在当前目录及路径中按 COM、EXE、BAT 顺序搜索可执行文件。在找到与用户命令对应的可执行文件后 DOS 读取磁盘上的文件装入内存，装入内存的过程称为加载，加载后 CPU 从既定地址起执行装入内存的软件。

虽然 COM 和 EXE 都是可执行文件，但它们的结构和装入内存的方式是不一样的。COM 文件的长度不大于 64KB，DOS 把整个 COM 文件装入当前可用内存段，磁盘文件的开头对应于内存段偏移地址 100H 处，这也是加载后 CPU 开始执行指令的地址。一个正确的 COM 文件从它的开始处就必须是合法的 CPU 指令。反之如果一个磁盘文件的扩展名是 COM，而它的开头不是合法 CPU 指令，当用户打入文件名时 DOS 仍会把它当成命令文件来加载，但由于加载后 100H 处指令不会

产生死机等异常现象。EXE 文件的结构和装入过程比 COM 文件复杂得多，文件长度可以超过 64KB，加载后的起始执行地址由 EXE 文件中的特定数据确定。总之不论是 COM 还是 EXE 文件，加载运行过程都是把磁盘文件读出装入内存，再从某个起始地址起执行软件。

二、可执行文件的退出与驻留

驻留内存是文件型病毒的一个重要特性，为了深刻了解病毒驻留的含义，我们先分析可执行文件的退出与驻留问题。

细心思考一下我们所用过的大量软件，会发现有两种运行情况。一种情况如字编辑软件 WS.COM，在运行过程中它占用微机内存，用户要结束编辑工作可以用 X 命令退出，退出后 WS 的工作当然中止了，同时也让出了它在运行过程中所占用的全部内存，或者说是释放了内存。磁盘上大部分软件的工作情况与 WS 是一样的，整个运行过程可以总结成：

1.用户打入文件名回车后加载可执行文件到微机内存中，占用全部或一部分可用内存；

2.从某确定地址起执行内存中的软件，实施软件的功能，如字处理、辅助设计、教学、游戏等；

3.退出软件运行中止功能，并且让出软件所使用的全部内存。

磁盘上另有为数不多但具有重要特殊功能的文件，它们的运行情况与 WS 软件不太相同，比如 QZCD.EXE、HAN.EXE、GB4.EXE 等等。当用户打入这些文件的主文件名执行它们的时候，都是只显示一个彩色图案后就立即回到 DOS 提示符下，也就是这些软件的功能并不是在加载它们的当时体现出来的，而是在这些软件执行后继续使用微机的过程中体现出来的。它们的功能是：

QZCD.EXE“光盘伴侣”系统的主文件，执行这个文件后解决了光盘 CD-ROM 不可写入的问题，用户运行光盘软件的时候有自动写伴侣盘的功能。

HAN.EXE“英汉通双向辞典”的主文件，执行这个文件后用户可以

随时抓取屏幕上的中英文单词进行英汉和汉英双向翻译。

GB4.EXE“游戏克星”系统的主文件，执行这个文件后用户可以跟踪分析其它软件的运行情况。

不难理解，既然这些软件的主要功能是在它们的主文件执行后体现的，说明当主文件中止执行后，软件的全部或一部分并没有退出内存，而是留在内存中才能在微机运行过程中随时为用户提供相应的功能服务，这种情况叫做软件驻留内存。为使驻留软件能够正常运行必须事先做一些准备工作，适当合法地修改微机操作系统，使得在必要时去执行驻留软件。比如 HAN.EXE、GB4.EXE 的功能可以随时用热键呼出，QZCD.EXE 则自动实现不可写光盘与可写伴侣盘之间的读写转换。为驻留软件做准备的工作叫做驻留软件的初始化引导，而引导正是在可执行文件运行的时候完成的，所以具有驻留功能的文件执行过程是：

1.用户打入文件名回车后加载可执行文件到微机内存中，临时占用全部或一部分可用内存；

2.从某确定地址起执行内存中的软件，进行初始化引导为驻留作准备；

3.退出文件运行回到 DOS 提示符下，但文件的一部或全部作为驻留软件留在内存中，为微机的运行提供相应的功能服务。

驻留软件有两大特征，一是驻留软件都要占用一定量内存，使用内存检测软件在驻留软件运行前后各检查一次内存使用情况会发现可用内存减少了，就是被驻留软件占去一部分的缘故。在实现既定功能前提下占用内存当然越少越好，象 QZCD.EXE 驻留部分使用内存不到 1KB，非常短小，而防毒软件 VSAFE.EXE 占用 40 多 KB 就显得大了些。第二个特征是多数软件从开始驻留到微机关机，随时可以提供相应的功能服务。

除极少数特例外，绝大部分文件型病毒都驻留内存，当然病毒驻留不是为微机增加有用的新功能，恰恰相反是为了随时向用户发难。

3.2　文件型病毒

文件型病毒是计算机病毒的一大类别，它们寄生在可执行文件上，当用户运行软件的时候，文件型病毒随加载可执行文件进入微机内存，使微机内存带毒运行，伺机传染其它可执行文件，并且在条件满足时破坏微机信息资源。

一、文件型病毒的寄生形式

当出现磁盘上的可执行文件莫名其妙地加长了的情况时，往往就是病毒所为。绝大多数文件型病毒属于所谓外壳病毒，什么是文件外壳呢？简单地说是计算机软件的一种层次结构。比方说计算机软件公司编制了一种教育软件，经过设计调试，软件本身的功能已经很完善，可以作为独立的磁盘文件提供给用户。但为了提高产品的商品化程度，公司决定为软件加一个漂亮的封面，为此设计人员可以在已经完成的软件基础上附加一段显示封面的程序。通常我们称软件本身为内核，而附加的显示封面程序称为外壳，加载运行关系见图 3-1。

图 3-1(C)表明尽管在结构上外壳接在内核后面，但运行的顺序仍然是先显示封面再跳转去执行内核。

可执行文件的外壳一般具有相对独立的功能和结构，去掉外壳将不会影响内核部分的运行。去外壳在有些情况下是有用的，比如有一种"脱壳解密"软件，其功能就是脱去加密软件的附加外壳，还原未加密的内核部分。

如果我们用"病毒外壳"去替换图一中的"封面外壳"，那么就已经说明了文件型病毒的最基本机理。文件型病毒是一段计算机程序，它们通过传染附着在可执行文件上。文件型病毒的寄生方式有：

1.大多数文件型病毒附着在可执行文件尾部，如图 3-1(C)。

2.少数文件型病毒附着在可执行文件前部，如图 3-1(B)。

3.幽灵病毒的主要部分附着在文件尾部，但另有十段小程序随机

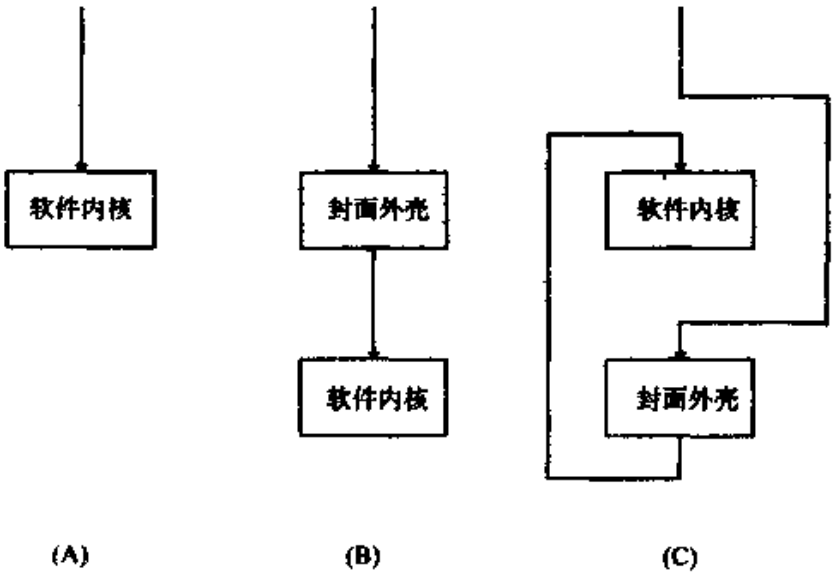


图 3-1 外壳和内核的加载运行

(A) 无外壳 (B) 外壳加载内核前面 (C) 外壳接在内核后面

地插入到被传染的文件中间。

4.RS232、1855 等病毒插入到文件的"空闲"部位。

5.DIR-II 的寄生方式比较特殊,整个磁盘只有一个病毒体,寄生在磁盘的最高簇。

二、文件型病毒的安装驻留

当用户运行软件的时候,如果可执行文件带有病毒,则病毒作为文件的一部分随文件加载到内存中。病毒首先根据动态标志判断内存中有无同一病毒在活动,如果病毒已由此前运行其它文件带入内存,就直接去运行原文件,反之病毒将开始安装。

文件型病毒可以象引导型病毒一样安装在基本内存高端,也可以利用 DOS 的内存管理功能占用一个内存块,被占用的内存块通常可以用内存检测软件检查出来。除 VIENNA 等很少数特例外,文件型病毒都采用驻留技术让病毒赖在内存中,不随应用软件退出。

绝大多数文件型病毒修改 INT 21 中断以备传染其它文件,但国内

也发现了几个修改 INT 2F 的病毒，DIR-II 病毒则不利用中断，而是修改设备驱动程序。

三、文件型病毒的传染机理

文件型病毒通过与磁盘文件有关的操作进行传染，主要途径有：

1.加载执行文件

文件型病毒驻机后，通过其所截获的 INT 21 中断检查每一个加载运行的 COM 和 EXE 文件进行传染。在 DOS 内部加载执行文件是由 INT 21 的 4B 调用实现的。国内已经发现截获 INT 2F 传染病毒，从系统内部看 INT 2F 与 INT 21 的 4B 功能完全不同，但从病毒传染过程的表象看两者类似，只是 INT 2F 需判断用户输入的字符命令是否为可执行文件名。

加载传染方式每次传染一个文件，即用户准备运行的那个文件，传染不到那些用户没有使用的文件。

2.列目录过程

一些病毒编制者可能感到加载传染方式每次传染一个文件速度较慢，不够过瘾，于是后来造出通过列目录传染的病毒。

在用户列硬盘目录的时候，病毒检查每一个文件的扩展名，如果是 COM 或 EXE 文件就调用病毒的传染模块进行传染。这样病毒可以一次传染硬盘一个子目录下的全部可执行文件。DIR 是最常用的 DOS 命令，每次传染的文件又多，所以病毒的扩散速度很快，往往在短时间内传遍整个硬盘。

对于软盘而言，由于读写速度比硬盘慢得多，如果一次传染多个文件所费时间较长，容易被用户发现，所以病毒"忍痛"放弃了一些传染机会，采用列一次目录只传染一个文件的方式。

3.创建文件过程

创建文件是 DOS 内部的一项操作，功能是在磁盘上建立一个新文件。已经发现利用创建文件过程把病毒附加到新文件上去的病毒，这种传染方式更为隐蔽狡猾。因为加载传染和列目录传染都是病毒感染

磁盘上原有的文件，细心的用户往往会发现文件染毒前后长度的变化，从而暴露病毒的踪迹。而创建文件的传染手段却造成了新文件生来带毒的奇观。好在一般用户很少去创建一个可执行文件，但经常使用各种编译、连接工具的计算机专业工作者应该注意文件型病毒发展的这一动向，特别在商品软件最后生成阶段严防此类病毒。

3.3 PRG 文件杀手病毒分析

PRGKILL 是一个典型的文件型病毒，大约 1995 年春季在西北地区首先被发现。病毒虽然并不复杂，危害却很严重。它自称是“PRGKILLER”，即“PRG 文件杀手”，一旦激发将破坏各种数据库中扩展名为 PRG 的全部程序文件，造成数据库瘫痪。

PRGKILL 长度 1024 字节，传染可执行 COM 文件和攻击数据库 PRG 文件。病毒的指令代码没有加密，但有两段加密的字符串，一段位于病毒偏移 3E4H，密钥是 03，解密后为“C:\COMMMAND.COM”，专为传染 DOS 命令文件而用；另一段从病毒偏移 360H 起，长 A0H(10 进制 160)字节，密钥 33H，解密后是一段短文：

This program is designed for the lady .....

Now, Thank you use this program. PRGKILLER

大意是：本程序(病毒)献给某某女士，感谢你使用这个程序...PRG 杀手。

病毒通过加载运运行带毒软件进入内存，利用直接改写内存链和 PSP 中的有关单元来侵占内存，驻留后占用基本内存高端 500H 字节，其中前 400H 是病毒体，后 100H 是文本数据区。用 MI 等软件查不到病毒的驻留现象，只能计算内存总量才会发现少了 500H 字节。病毒修改 DOS 调用 INT 21 中断地址指向病毒段的 0266H 偏移处。PRGKILL 检测驻机的动态标志是用 AX = EE02H 调用 INT 21，如病毒驻机则对 AX 取反后返回 AX = 11FDH，否则表示病毒未驻机。

每当用户使用 DIR 命令，病毒都监视操作目录下的全部 COM 和

PRG 文件。对于 COM 文件病毒将检查文件的时间秒值，如果计数低 4 位为 0AH，则认为文件已经感染 PRGKILL 病毒，不重复传染。否则病毒把自己加在原文件尾部，使文件增长 1024 字节，并且修改文件时间秒计数低 4 位成 0AH 作为染毒标志。对于硬盘上的 COMMAND.COM 文件病毒在第一次侵入微机时立即传染。为了使运行染毒文件时首先执行病毒部分，病毒在传染的时候把原文件的前三字节改成转移到病毒的跳转指令。原文件的前三个字节保存在病毒体的前三个字节中，病毒开始运行后将把这三个字节移回文件开头。

在列目录过程中遇到 PRG 文件，病毒检查系统日期，如果开机日期是任意月份的 1 号，病毒将破坏性改写 PRG 文件，方式是把关于“杀手”的 160 字节短文写到 PRG 文件的起始处，同时向文件的其余空间填入无意义的任意数据，从而彻底破坏 PRG 文件。但对于长度大于 65535 字节的 PRG 文件病毒将不予处理。

病毒采用了隐身手段，在列目录的时候把染毒文件的长度减去 1024 字节显示给用户看，使用户看不出染毒文件长度的变化。

一、安装模块

下页是 PRG 文件杀手病毒的传染模块。

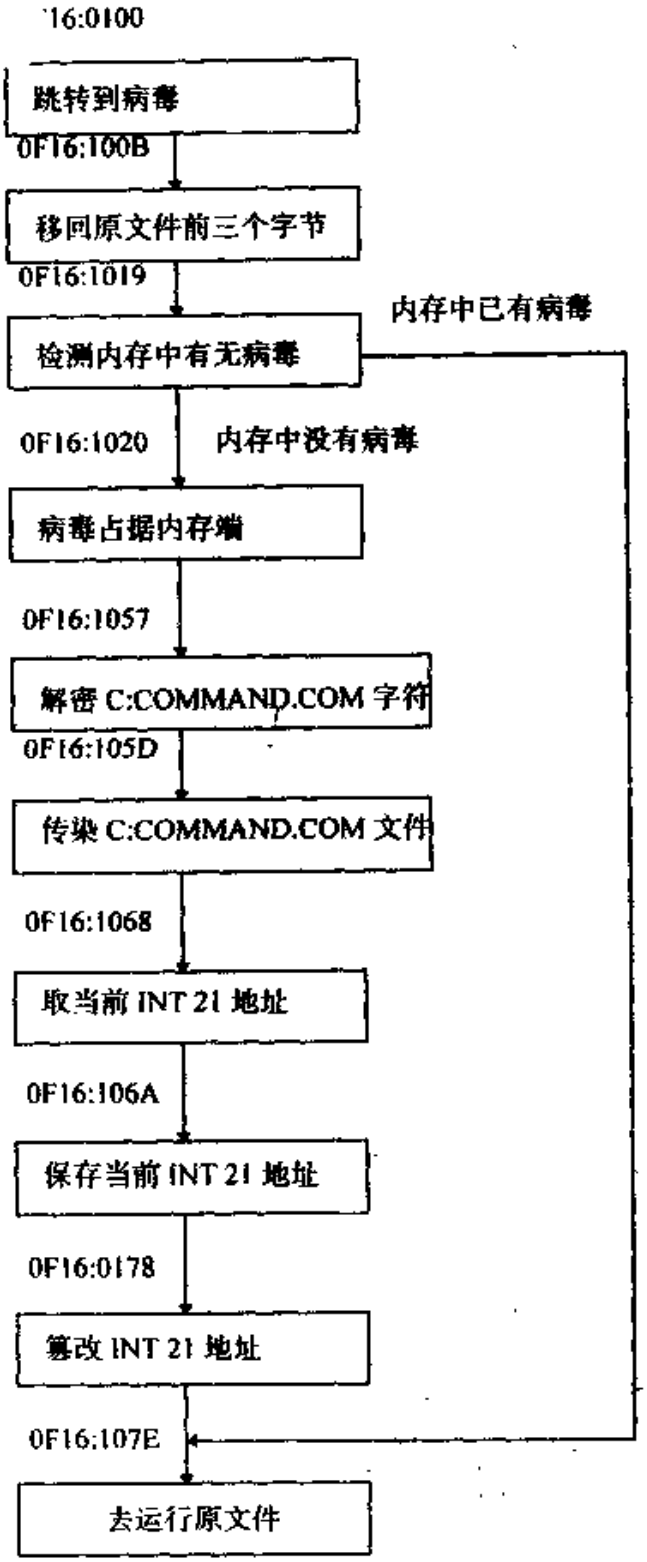
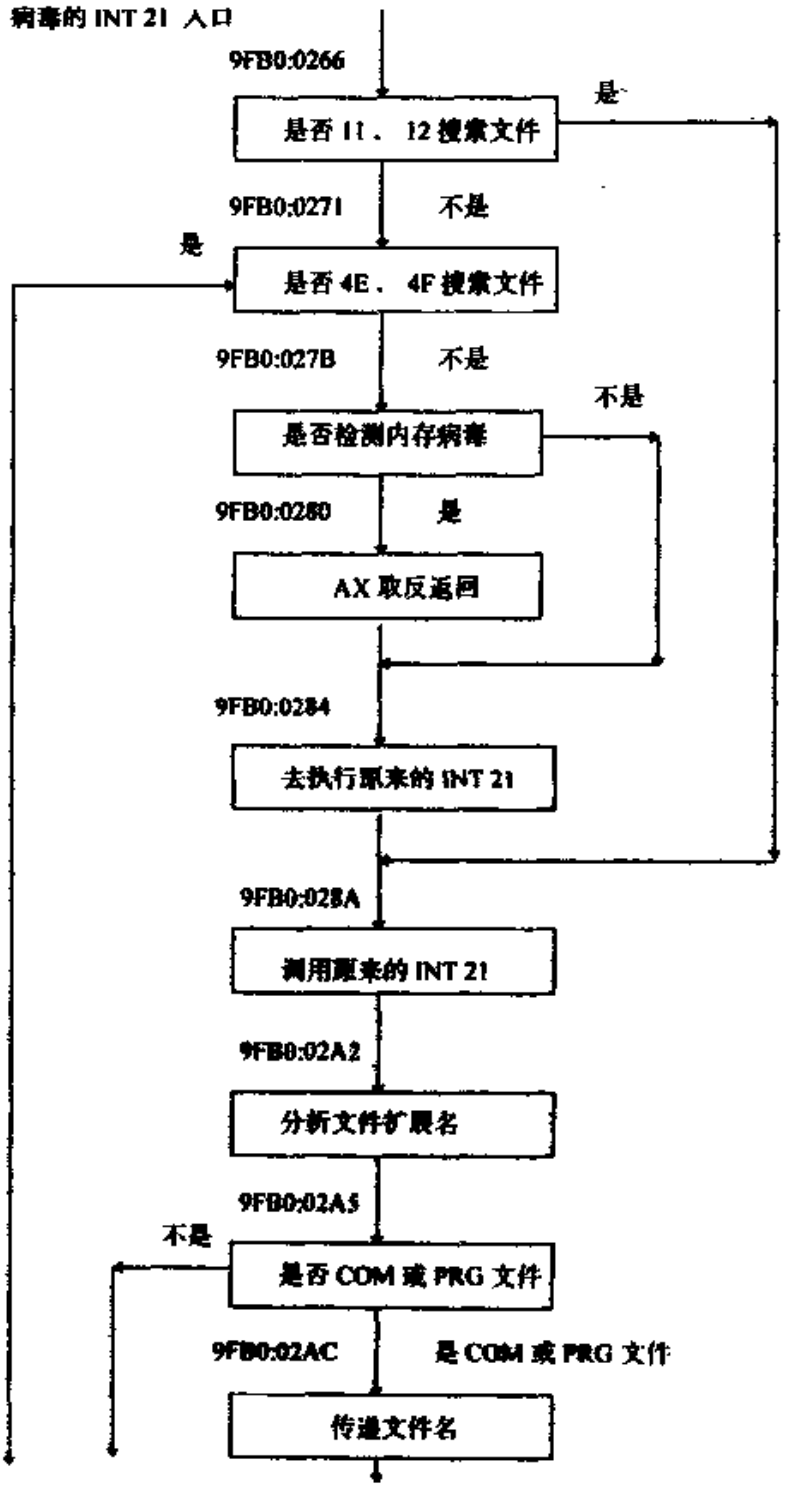
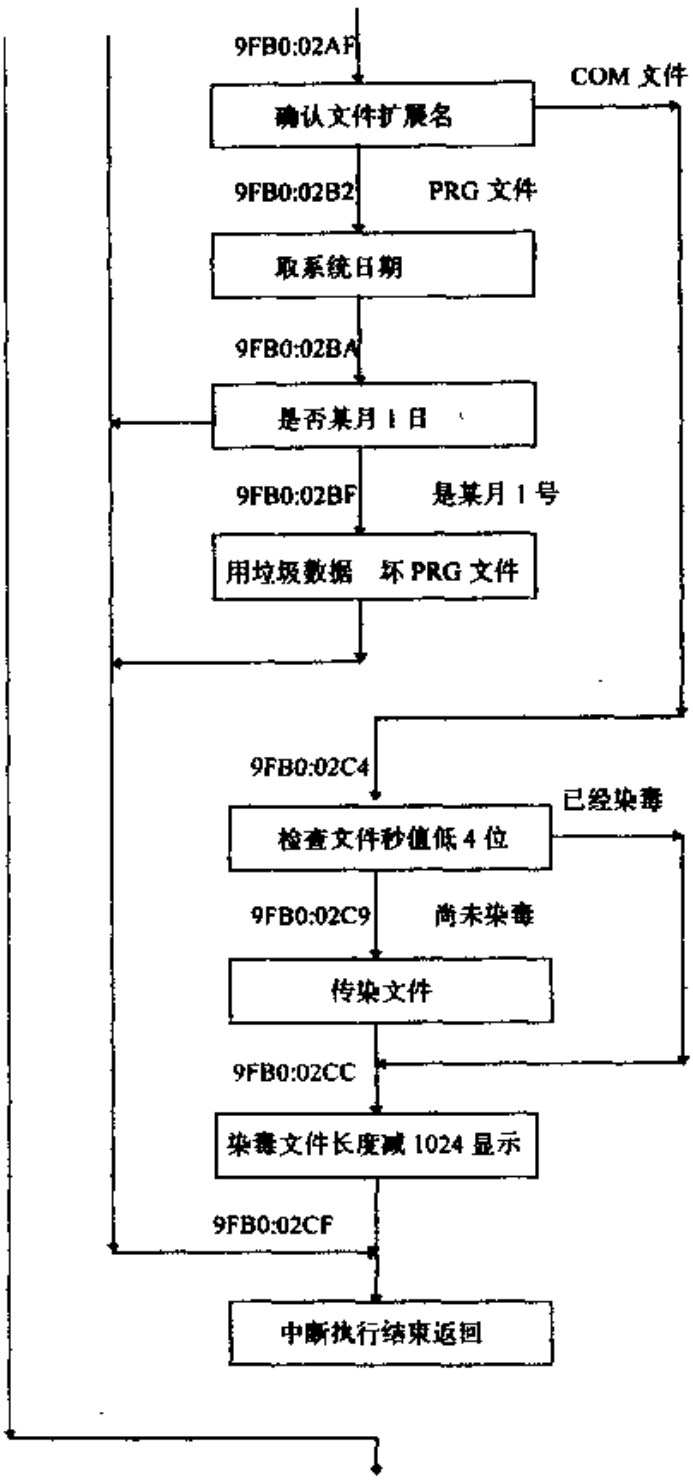


图 3-2 PIC 文件杀手病毒的传染模块

二、传染破坏模块


病毒的 INT 21 入口
9FB0:0266
是否 11、12 搜索文件
是
9FB0:0271
不是
是否 4E、4F 搜索文件
是
9FB0:027B
不是
是否检测内存病毒
不是
9FB0:0280
是
AX 取反返回
9FB0:0284
去执行原来的 INT 21
9FB0:028A
调用原来的 INT 21
9FB0:02A2
分析文件扩展名
9FB0:02A5
是否 COM 或 PRG 文件
不是
9FB0:02AC
是 COM 或 PRG 文件
传递文件名


9FB0:02AF
确认文件扩展名
COM 文件
9FB0:02B2
PRG 文件
取系统日期
9FB0:02BA
是否某月 1 日
9FB0:02BF
是某月 1 号
用垃圾数据 坏 PRG 文件
9FB0:02C4
检查文件秒值低 4 位
已经染毒
9FB0:02C9
尚未染毒
传染文件
9FB0:02CC
染毒文件长度减 1024 显示
9FB0:02CF
中断执行结束返回

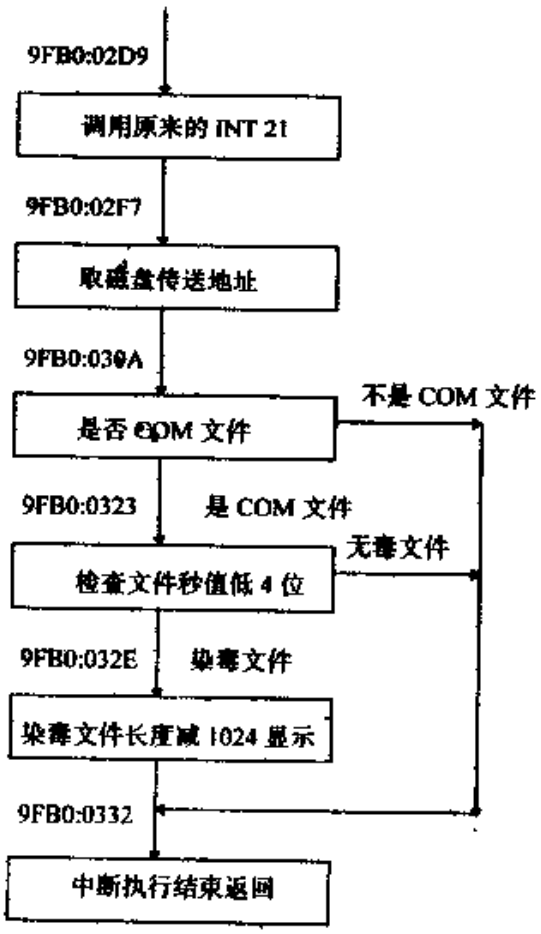


图 3-3　PRG 文件杀手病毒的传染和破坏模块

3.4 混合型病毒

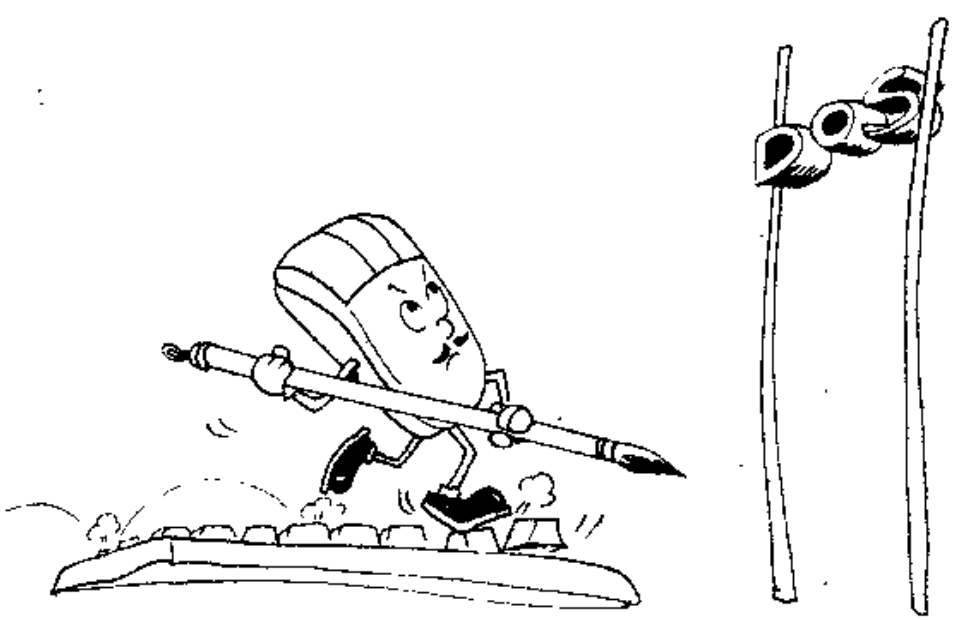
混合型病毒是引导型病毒和文件型病毒的混血儿，又称双料病毒，既传染可执行文件，又传染磁盘引导区。国内已经发现的混合型病毒有 FLIP、ALFA、NATAS、幽灵、秋水等。从病毒基本原理上说混合型病毒没有什么新的突破，上面关于引导型病毒和文件型病毒的分析也分别适用于混合病毒的引导部分和文件部分。但混合型病毒两部分之间遥相呼应互为犄角，更难防御，因此要注意它们的一些新特点。

混合型病毒比较长，比如 FLIP 长 2153 字节，幽灵长 3544 字节。一般不传染软盘引导区，当使用外来软盘上的染毒可执行文件时，病毒进入微机并立即传染硬盘引导区。此后每次开机病毒都进驻内存，所占用的内存量比单纯引导型病毒更大。因为加载引导区时 DOS 系统尚未建立，所以病毒还要通过 INT 08 或 INT 1C 调用监视引导过程，等 DOS 系统建立后予以修改，以便在微机工作过程中传染可执行文件。如果由于某种原因，混合型病毒未能在开机引导过程中驻留内存，比如用无毒系统软盘引导微机或者硬盘引导区病毒被杀除，但硬盘很多文件仍然带毒，只要运行任何一个带毒文件病毒就会再次驻机。

对于混合型病毒必须同时检测杀除引导区和可执行文件中的病毒才能彻底根治，否则若只杀文件病毒不杀引导病毒，或者只杀引导病毒不杀文件病毒，则混合病毒都会很快复发。

第四章

计算机病毒的预防和诊治



计算机病毒的危害是人所共知的，每一位用户都希望自己的计算机安全使用，免受计算机病毒的攻击，这就要做好反病毒工作。反病毒包括计算机病毒的预防和诊治两个方面，可以分为三个层次：

1.预防计算机病毒侵入微机。

2.在病毒传染阶段消除病毒。

3.病毒激发后的挽救工作。

4.1 计算机病毒的传染途径与外来软件

计算机病毒是人为编制的特殊软件，通过信息共享逐渐转播。一台没有病毒的微机感染计算机病毒的唯一途径是使用了带毒的外来软件。那么从反病毒观点来看哪些软件属于“外来”呢？主要有下列几种：

1.通过磁盘拷贝得到的自由软件和共享软件

这是计算机用户获得软件的主要来源之一。此类软件往往经过多台微机多次拷贝，感染病毒的几率较大，有时病毒还会交叉感染，是计算机病毒的主要传播途径。

2.用户新购入的商品软件

有一种观点认为花钱买来的软件不会有病毒，这是有害的。因为首先在有些情况下虽然用户花费了钱财，但得到的并不一定是正规产品。社会上有些人以赢利为目的出售非版权软件，还有些计算机硬件产品配套不全，由销售商自行拷贝配套软件供给用户，这些都是计算机病毒的潜在传播媒介。95 年发现一种声霸卡的驱动程序软盘带有 EXEBUG 和幽灵两种病毒。其次大公司出售的正版软件带毒可能性相对较小，但也不能把话说绝。90 年代初发生过台湾某公司出品的微机操作系统带毒问题。95 年有用户投书计算机专业媒体，反映某大软件公司出售的正版软件质量差，含火矩恶性病毒和 BUPT 病毒。

3.一些行业部门自行开发，在本系统应用的软件

这类软件通常由行业主管部门组织开发，在本系统内推广应用。

“下级”用户往往认为软件来源于“上级”部门，不会有什么问题。但此类软件多是用工具软件编制的，设计人员可能不特别关注更低层的病毒问题。92 年南方某大城市的银行曾研制一套财务软件，通过带写保护的软盘提供给下属数百个单位使用，正是该软盘带 2708 恶性病毒造成很多单位微机数据破坏。

4.用户的磁盘借出后又归还

借出的软盘总要在他人微机上使用，归还时已具有“外来”软件的性质。

5.使用网络服务器上的软件

服务器是网络用户的共享设备，某用户在某时刻使用某软件是无毒的并不能保证下一次使用该软件仍然无毒，因为其他用户可能对服务器进行读写致使软件染毒。

4.2　防止计算机病毒侵入微机的预防措施

防止计算机病毒侵入微机的关键是把好外来软件关，宜采用加强安全管理和技术手段检测双管齐下的措施。在管理方面对于专用微机来说应该坚持不使用和少使用外来软件的原则。机关团体企事业单位的一些专用微机用途比较固定，而且多半担负重要工作，应该特别注意安全问题。某大单位专用于工资管理的微机曾因有人玩游戏染上病毒造成数千职工工资不能按时发出，所以专用机必须严格管理限制外来软件的使用。其它管理措施还包括设置密码、控制使用权等。

对于大量通用性微机而言，笼统地说不使用外来软件既于事无补，也不可能。因为软件信息共享是现代计算机的精髓，从一定意义上说微机引入的软件越多，其效益就越高，一位初学者正是通过大量引入各种软件而成为计算机高手。所以从计算机安全角度考虑应该注重外来软件使用前的检测工作。

1.在运行外来软件前使用查毒杀毒工具对外来软件进行检测杀毒。查毒杀毒工具的用法一般用户都知道，但应该注意现在很多软件

在软盘上是以压缩或者镜像文件格式存储的，需要解压缩或释放到硬盘上使用。对于这些软件应该先检查一次软盘，然后安装到硬盘，再检测一次硬盘。由于压缩和镜像文件的特殊机理，不排除检测软盘无毒而安装到硬盘上的软件带毒现象，所以有必要软盘硬盘各检测一次。可以放心，当软盘上的安装文件无毒时，那么由该安装文件把软件解压缩或释放到硬盘上，即使安装后的硬盘软件带毒，只要不运行它就不会波及硬盘其它软件。所以安装后运行前是检查病毒的正确时机。

2.对于第1项没有查出病毒，但来路很没有把握的软件，比如用户之间交流软件，有时一方会提醒另一方："小心！软盘可能有病毒"，有必要进一步检查。方法是第一次运行外来软件的时候，一进入运行状态就立即退出。比如很多游戏软件显示画面的时候都有结束游戏的选择，可立即选择此项。退出后操作一下诱饵软盘(见本章第三节)，并用下面介绍的各种方法检查诱饵盘是否被病毒传染。

3.使用防病毒工具。如果外来软件含有杀毒工具查不出的新病毒，那么借助于防病毒工具有可能防止新病毒的传染破坏。在这种情况下，新安装到硬盘上的软件是带毒的，也就是说微机已经带毒，防病毒工具的作用是不让病毒传染硬盘的其它部位。由于微机带毒不宜无把握地继续运行，应及时找反病毒部门或专业技术人员处理。

4.对于纯引导型病毒而言，唯一感染微机的途径就是用带毒软盘启动微机，所以只要养成良好的防病毒习惯，坚持不用软盘启动微机就能有效地把引导型这一大类病毒拒于微机门外。实际上除非有特殊需要，现在很多用户已习惯于在开机上电时不用软盘，问题往往发生在开机后在软驱中插入带毒盘片(包括非系统数据盘)，而用 RESET 或 CTRL-ALT-DEL 复位时忘记取出软盘，会造成带毒引导，这是应把好的关口。现在很多微机可以设置引导盘的优先顺序，设 C 盘优先是防治引导病毒的一个好方法。

4.3　计算机病毒的检测

检测病毒是处理计算机病毒的前提，检测的方式有自动检测和人工检测之分。自动检测是指使用专用反病毒工具，包括查杀毒软件、集成消病毒卡和防病毒卡等，它们都是专业产品，使用方便，有较强的查毒、杀毒、防毒能力。但病毒防范具有较强的时效性，专用产品不能包揽一切，所以人工检测还是有必要的。人工检测是由用户根据微机运行过程中的一些异常想象，使用 PCTOOLS、DEBUG、MEM、MI 等通用工具软件检测病毒的方法。为了安全准确地诊治计算机病毒，平时准备好下面两种软盘是有必要的：

一、系统软盘

通常用户认为微机有染毒迹象时进行病毒检测，在这种情况下继续使用硬盘是危险的，所以平时应准备好干净的系统软盘。系统软盘可在微机无毒情况下用带/S 参数 FORMAT 命令制作。软盘上应该有 PCTOOLS、DEBUG、MEM、MI 、NORTON 等工具软件。软盘尽可能不用 CONFIG.SYS 和 AUTOEXEC.BAT 文件，如果必须有这两个文件，则它们所涉及到的其它文件应该在软盘上找到。系统软盘应该处在严密的写保护状态下。

在微机硬盘带毒或者怀疑染毒情况下，用无毒系统软盘启动微机，并且不运行硬盘上的软件，可以保证微机内存中无毒，以便用软盘上的 DEBUG 、PCTOOLS 工具观察硬盘有关扇区和文件，进行静态病毒分析。

二、诱饵软盘

格式化一片软盘，把几个用户熟悉常用的可执行文件拷贝到软盘上，记下软盘上各个文件的长度、日期、时间以及软盘的剩余空间和卷标，用 DEBUG 打印出引导区数据(或作为一个数据文件保存)即可作为

诱饵盘使用。

诱饵盘是"舍己为人"的战士,在诊断病毒的时候可以故意用诱饵盘引诱病毒传染,因为诱饵盘的重要数据和文件是已知的,所以能准确快速地判断病毒。

当怀疑微机内存中有病毒活动时,应该停止硬盘操作,在软驱中插入诱饵盘。用 DIR 命令对诱饵盘列目录可以诱发引导型病毒和 109X、DABI 等 DIR 类文件型病毒传染;运行可执行文件可以诱发 DOGLAS、1167 等执行类文件型病毒传染。传染过后即可用无毒系统软盘引导微机,从容地对诱饵盘的引导区和可执行文件进分析。

4.4 检测引导型病毒

一、内存检测

在引导型病毒加载安装的时候,微机内存管理机制刚刚开始建立,病毒得以占用的内存区域和可利用的系统资源十分有限。绝大多数病毒只能把自己安装在基本内存高端,并且只能通过修改内存 0 段 413、414 单元的内存容量值使其占用合法化,所以可通过检查 413、414 单元的内存容量值来检测引导型病毒。内存容量在 1 兆及以上的微机基本内存容量都是 640K,用 16 进制表示为 280。大多数微机开机后 413、414 单元就是这个值;个别机型如 COMPAQ,系统占用 1K,该值为 27F,还有大容量硬盘驱动程序可能占去部分内存。不论哪种情况都可预先记录 413、414 单元值,当怀疑微机有病毒时检查该两单元值。检查时应临时屏蔽 CONFIG.SYS 和 AUTOEXEC.BAT 文件(可临时改为其它名称,检查后再改回),以避免个别后加载文件的影响。如果该两单元值比正常记录值小,则感染引导型病毒可能性很大,减小的数值正是病毒占用的内存 K 数。

二、现象观察

1.如果微机硬盘可以引导启动,出现 DOS 引导符后 C 盘及各逻辑

盘工作正常，但用与硬盘 DOS 版本相同的无毒系统软盘引导出现 DOS 提示符后找不到硬盘上的正确文件，如 DIR 显示的文件名面目全非，则可以肯定硬盘主引导区染毒。特别请注意此时硬盘数据基本完好，应设法消除病毒，千万不要对硬盘重新分区。

2.引导型病毒传染软盘的机理是每次读写软盘病毒都要趁机读出软盘的第一个扇区判断是否染毒。因此可以用 DEBUG 或 PCTOOLS 读软盘一个编号较高的扇区，软盘驱动器工作灯熄后对该扇区再读一次。正常情况下驱动器只是灯亮一下再熄掉，听不到明显的声音；反之如果驱动器发出比较刺耳的寻道声，则可判定为是引导型病毒在寻找软盘 0 道。

3. 在用软盘引导微机的时候硬盘工作灯一般亮两次。第一次是在 ROM-BIOS 阶段测试微机硬盘；第二次是在 DOS 引导阶段读硬盘主引导区和 DOS 引导区获得硬盘参数，两次灯亮之间的间隔较长。如果用软盘引导微机的时候硬盘工作灯亮三次，其中前两次离得很近，则第二次灯亮是病毒在读硬盘引导区。

三、数据比较

对于怀疑引导区染毒的磁盘可以通过简单直观的静态比较法检测其引导区是否正常。比较法是拿怀疑染毒的引导区与正常无毒引导区进行数据比较。

软盘 DOS 引导区分为 DOS 3 和 DOS 5 两种版本，DOS 5 也用于 DOS 6。另外用 PCTOOLS、HDCOPY 等工具格式化盘的时候会产生特殊引导区，一般不宜做系统引导盘。DOS 引导区的版号和格式化时使用的工具通常可以在引导区的开头看出来。当怀疑软盘引导区染毒时可以将其与同版本同容量正常软盘的引导区进行比较，下面是用 DEBUG 比较两片软盘引导区的操作：

读 A 驱动器中无毒软盘引导区到内存 7C00 地址：

L 7C00 0 0 1

取出 A 驱动器中的无毒软盘，插入怀疑染毒的软盘，读软盘引导

区到内存 1000 地址：

L 1000 0 0 1

比较两个引导区的数据：

C 7C00 7DFF 1000

图 4-1 和图 4-2 分别是正常引导区和病毒引导区，可以看出从第 2 个字节起就不一样。

对于硬盘来说，当怀疑主引导区染毒时，可优先考虑与另一台同型号无毒微机主引导区进行比较；如果没有同型号微机，可以与其它无毒微机主引导区比较，绝大多数微机所配 540 兆以下硬盘的主引导程序是相同的。

DEBUG 和 PCTOOLS 都不能直接读硬盘主引导区，但读取主引导区的程序极为简单，完全可以在 DEBUG 下临时输入：

0100 MOV AX,201

0103 MOV BX,7C00

0106 MOV CX,1

0109 MOV DX,80

010C INT 13

010E INT 3

这段小程序用于把硬盘主引导区读到内存 7C00 地址。

```
7C00  EB 3C 90 4D 53 44 4F 53-35 2E 30 00 02 01 01 00    .<.MSDOS5.0.....
7C10  02 E0 00 40 0B F0 09 00-12 00 02 00 00 00 00 00    ...@............
7C20  00 00 00 00 00 00 29 F8-0F 50 36 4E 4F 20 4E 41    ......)..P6NO NA
7C30  4D 45 20 20 20 20 46 41-54 31 32 20 20 20 FA 33    ME    FAT12   .3
7C40  C0 8E D0 BC 00 7C 16 07-BB 78 00 36 C5 37 1E 56    .....|...x.6.7.V
7C50  16 53 BF 3E 7C B9 0B 00-FC F3 A4 06 1F C6 45 FE    .S.>|.........E.
7C60  0F 8B 0E 18 7C 88 4D F9-89 47 02 C7 07 3E 7C FB    ....|.M..G...>|.
7C70  CD 13 72 79 33 C0 39 06-13 7C 74 08 8B 0E 13 7C    ..ry3.9..|t....|
7C80  89 0E 20 7C A0 10 7C F7-26 16 7C 03 06 1C 7C 13    .. |..|.&.|...|.
7C90  16 1E 7C 03 06 0E 7C 83-D2 00 A3 50 7C 89 16 52    ..|...|....P|..R
7CA0  7C A3 49 7C 89 16 4B 7C-B8 20 00 F7 26 11 7C 8B    |.I|..K|. ..&.|.
7CB0  1E 0B 7C 03 C3 48 F7 F3-01 06 49 7C 83 16 4B 7C    ..|..H....I|..K|
7CC0  00 BB 00 05 8B 16 52 7C-A1 50 7C E8 92 00 72 1D    ......R|.P|...r.
7CD0  B0 01 E8 AC 00 72 16 8B-FB B9 0B 00 BE E6 7D F3    .....r........}.
7CE0  A6 75 0A 8D 7F 20 B9 0B-00 F3 A6 74 18 BE 9E 7D    .u... .....t...}
7CF0  E8 5F 00 33 C0 CD 16 5E-1F 8F 04 8F 44 02 CD 19    ._.3...^....D...
7D00  58 58 58 EB E8 8B 47 1A-48 48 8A 1E 0D 7C 32 FF    XXX...G.HH...|2.
7D10  F7 E3 03 06 49 7C 13 16-4B 7C BB 00 07 B9 03 00    ....I|..K|......
7D20  50 52 51 E8 3A 00 72 D8-B0 01 E8 54 00 59 5A 58    PRQ.:.r....T.YZX
7D30  72 BB 05 01 00 83 D2 00-03 1E 0B 7C E2 E2 8A 2E    r..........|....
7D40  15 7C 8A 16 24 7C 8B 1E-49 7C A1 4B 7C EA 00 00    .|..$|..I|.K|...
7D50  70 00 AC 0A C0 74 29 B4-0E BB 07 00 CD 10 EB F2    p....t).........
7D60  3B 16 18 7C 73 19 F7 36-18 7C FE C2 88 16 4F 7C    ;..|s..6.|....O|
7D70  33 D2 F7 36 1A 7C 88 16-25 7C A3 4D 7C F8 C3 F9    3..6.|..%|.M|...
7D80  C3 B4 02 8B 16 4D 7C B1-06 D2 E6 0A 36 4F 7C 8B    .....M|.....6O|.
7D90  CA 86 E9 8A 16 24 7C 8A-36 25 7C CD 13 C3 0D 0A    .....$|.6%|.....
7DA0  4E 6F 6E 2D 53 79 73 74-65 6D 20 64 69 73 6B 20    Non-System disk
7DB0  6F 72 20 64 69 73 6B 20-65 72 72 6F 72 0D 0A 52    or disk error..R
7DC0  65 70 6C 61 63 65 20 61-6E 64 20 70 72 65 73 73    eplace and press
7DD0  20 61 6E 79 20 6B 65 79-20 77 68 65 6E 20 72 65     any key when re
7DE0  61 64 79 0D 0A 00 49 4F-20 20 20 20 20 20 53 59    ady...IO      SY
7DF0  53 4D 53 44 4F 53 20 20-20 53 59 53 00 00 55 AA    SMSDOS   SYS..U.
```

图 4-1　正常 DOS 引导扇区(3 英寸高密盘 DOS 5)

```
1000  EB 39 90 4D 53 44 4F 53-35 2E 30 00 02 01 01 00    .9.MSDOS5.0.....
1010  02 E0 00 40 0B F0 09 00-12 00 02 22 00 00 EA 91    ...@.....".....
1020  99 00 F0 B8 01 02 B9 0E-00 BA 00 01 BB 00 06 CD    ................
1030  13 C6 06 1D 7C 00 EA 4D-06 00 00 FA 33 C0 8E D0    ....|..M....3...
1040  BC 00 7C 8E D8 8E C0 50-50 50 FB EB D6 37 1E 56    ..|....PPP...7.V
1050  16 53 BF 3E 7C B9 0B 00-FC F3 A4 06 1F C6 45 FE    .S.>|.........E.
```

图 4-2　含 BUPT 病毒的软盘引导扇区

4.5　消除引导型病毒

一、消除软盘引导型病毒

在判定软盘引导区感染引导型病毒后可以用简单的覆盖法消除病毒，操作步骤如下：

1.取与染毒盘同容量同格式的无毒软盘，比如染毒盘是用 DOS 6.2系统 FORMAT 命令格式化的 3 英寸 1.44M 盘，无毒盘应与其相同。对于非系统盘可以放弃格式化版本要求，只取同容量软盘即可。把选好的无毒盘插入驱动器，设为 A。

2.运行 PCTOOLS 工具，依次击 F3、E、A 键，屏幕上将显示出无毒盘的引导扇区。

3.取出无毒盘，插入染毒盘，依次击 F5、U 键即杀除了软盘引导区病毒。

二、消除硬盘主引导区病毒

硬盘引导区是整个硬盘最重要的部位，其代码数据正确与否直接关系到硬盘能否正常工作。因此对于人工消除硬盘引导病毒要取辩证的态度。

首先既然硬盘引导区十分重要，最好在微机无毒的情况下预先备份。一些现成的反病毒工具如 CPAV、求真消病毒卡等都具有硬盘引

导区备份功能。当引导区不幸染毒时，用备份覆盖病毒是最可靠的杀毒方法。

其次反病毒工具已经很普及完善，毕竟是专业厂家的产品，自动化杀毒程度较高，较之人工现场操作要可靠得多，应尽量优先选用反病毒产品杀毒。

第三凡事都怕万一，如果既没有备份，又没有合用的杀毒产品，能不能人工杀毒呢？答案是在大多数情况下是可行的。在第二章中已经介绍硬盘主引导区由主引导程序和硬盘分区表两部分组成，由于技术上的原因大多数引导型病毒只修改主引导程序，但不修改分区表，也不移动分区表的位置。即主引导扇区的前部是病毒引导程序，后部仍是合法的分区表，病毒寄生情况及杀毒方法见图 4-3。

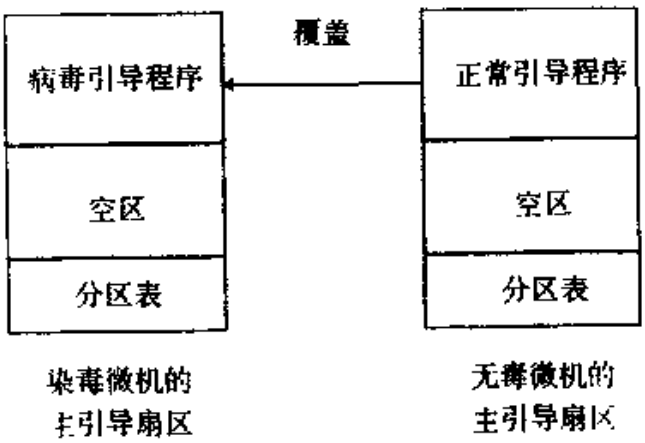


图 4-3　消除硬盘主引导区病毒

在杀毒前必须确认所遇到的病毒符合图 4-3 的描述，方法很简单，就是用无毒软盘引导微机，出现 DOS 提示符后依次进入 C、D、E 盘……，进行列目录操作，运行一两个常用软件，如果都正常，则染毒情况与图 4-3 相符；否则若出现不能进入硬盘，或者虽可进入硬盘但列目录错误，常用文件不能运行现象，则病毒寄生情况与图 4-3 不符。

在确认病毒寄生情况后，杀毒步骤如下：

1. 在无毒微机上运行 DEBUG，输入下列程序之后执行 G = 100，读取无毒主引导区到内存 7C00。

```
0100 MOV AX,201
```

0103 MOV BX,7C00

0106 MOV CX,1

0109 MOV DX,80

010C INT 13

010E INT 3

2.把无毒主引导程序作为数据文件保存在 A 驱软盘上,文件名为 MBP.DAT,长度为 190 个字节,16 进制 1BE。

R BX

0

R CX

1BE

N A:MBP.DAT

W 7C00

3.在染毒微机上运行 DEBUG,输入下列程序并运行,读取病毒主引导区。

0100 MOV AX,201

0103 MOV BX,7C00

0106 MOV CX,1

0109 MOV DX,80

010C INT 13

010E INT 3

4.从无毒微机驱动器中取出含 MBP.DAT 文件的软盘插入染毒机驱动器,读 MBP.DAT 文件覆盖病毒引导程序。

N A:BMP.DAT

L 7C00

5.修改第 3 步的第一行程序为 0100 MOV AX,301,执行 G=100 完成杀毒。

4.6　检测文件型病毒

一、检查磁盘剩余空间

当内存中驻留有文件型病毒的时候要对可执行文件进行传染，除DIR-II等极少数病毒，被病毒传染的文件长度都要增加，一般是数百字节到数K字节。但很多病毒为欺骗用户而采用了隐蔽技术，当这些病毒驻机时隐藏被它们传染文件的长度变化。另一方面文件长度增加意味着磁盘可用空间的减小，所以当怀疑内存中有文件型病毒活动时应密切注意操作盘的剩余空间容量，如果仅仅是由于列目录而造成磁盘空间减小，可以判定是文件型病毒传染作祟；如果执行一个文件，该文件本身没有存储操作而磁盘空间减小亦可得出同样结论。

二、检查可执行文件长度

在非用户操作下可执行文件长度增加肯定是病毒，但如前所述很多病毒驻机时隐藏了文件长度变化，机理是内存中的病毒监视DIR列目录操作，遇到可执行文件的时候根据病毒标志判断件是否染毒，如果染毒就减去病毒的长度显示，这样用户看到的将是原文件的长度。可见隐藏染毒长度变化的前提是病毒驻留内存。对症下药，用户可以用无毒软盘引导微机保证内存中没有病毒，用DIR命令列目录，染毒文件的长度变化将暴露无遗。

三、检查可执行文件是日期

磁盘上的每个文件都有日期和时间记录，用DIR命令列目录时屏幕上会显示年、月、日、小时和分，但不显示秒。准确地说文件的日期时间是指最后一次修改的日期时间。比如用微机写文章通常不会一次就写完，而是要多次补充和修改，DOS总是记录用户最后修改文章的日期时间。文件日期时间的变化记录在目录表中该文件目录项的第23到

26 字节中，见第二章第一节。

文件型病毒对可行文件的传染就是改写该文件，很多病毒采取在传染前保存文件原来的日期时间，传染后强行把原日期时间强行写回目录区，所以列目录时看不出日期时间的变化。但也有些病毒如 PRGKILL、VACSINA 等没有使用这种技术，染毒文件的日期时间被置成传染当时的日期时间，这可以做为检查此类病毒的依据之一。即列目录时发现一些可执行文件的日期变成最近的日期，说明这些文件已被病毒传染。

四、检查可执行文件是时间

一些病毒用磁盘目录表中的文件时间值做为感染标志，这种作法可能是病毒编制者随机决定的，但在下面两种情况下却有其技术背景：

1. 变形病毒每次传染的磁盘记录结果都不一样，很难用病毒本身代码作感染标志，不得不转用其它标志，时间则是其首选目标。

2. 列目录时隐藏长度变化的病毒不可能调出文件去检查文件中的代码标志（否则时间太长），而时间恰好是列目录过程需要的参数，所以病毒自然选时间作感染标志。

变形技术和列目录时隐藏长度变化都是病毒发展的方向，所以今后有可能出现更多用时间作标志的病毒。

为不暴露自己，病毒多选用列目录时不显示的秒值作标志。以秒值为标志的几个病毒例子：

VIENNA（维也纳）和 Casper 病毒置秒值为 62。

DOCTOR（医生）病毒置秒值为 60。

幽灵病毒置秒值等于日期除以 30 的余数。

当病毒选 0 到 58 秒为标志的时候不构成判断病毒的充分条件，因为一正常无毒文件的秒值也必定是 0 到 58 中的某一个数。但 62 和 60 秒是正常 DOS 操作不会出现的秒值（见第二章第一节），所以可以用 PCTOOLS 等工具观查磁盘目录表中的可执行文件秒值，若为 60 和 62 即可认为该文件被病毒感染。下面是 PCTOOLS 显示的某文件的目录

项：

44 45 42 55 47 20 20 20 43 4F 4D 20 00 00 00 00 DEBUG... COM.....

00 00 00 00 00 00 1E 60 30 0F B8 04 89 4E 00 00 .....N..

从中看出秒值是 16 进制 1E，相当于 10 进制 30，因秒值还需乘 2，所以目录表中的 1E 代表 60 秒，实际上这个 DOS3.31 的 DEBUG.COM 文件染有 DOCTOR 病毒。

由于秒的计数范围是有限的，包括两个非法数在内从 0 到 31 仅 32 个值，不同的病毒都用秒值作标志必然产生“撞车”现象，如上面列出的 VIENNA 和 Casper，从而造成病毒判断上的混乱，有时还使无毒文件的显示长度“减小”。

五、观察传染现象

文件型病毒在传染软盘文件的时候会有比较明显的征兆：

1.当对软盘列目录时如果有明显的停顿现象，并且驱动器发出寻道噪声，说明微机内有 DIR 类病毒正在传染文件。

2.除加密软盘外，软盘运行可执行文件时读盘声一般比较均匀，但内存中有病毒活动时往往跳跃读盘和写盘，驱动器运行声音明显增大。

3.用户没有向软盘上存文件，但屏幕上提示软盘写保护(Write protecterror writing drive A or B)是一些不完善病毒传染的表现。

硬盘速度很快，上述现象不明显，一般难以觉察。

六、指令代码比较

微机一旦染上文件型病毒会在短时间内传染硬盘上的很多文件，使原本并不相干的文件都附加上一个共同的外壳。因此可以用 DEBUG 检查各个常用子目录中的可执行文件头，如果都相同或相似，则很可能是感染了同一种病毒。在进行比较的时候要尽可能选相互之间没有关系的软件，比如说甲公司的游戏软件与乙公司的编辑软件，比较软件的关连度越小则判断的可信度越高。同一子目录下的文件往往属

于同一公司产品，可能采用相同的封面或加密外壳，不宜作为判别病毒的比较对象。

4.7 消除文件型病毒

文件型病毒为数众多，彼此之间差异较大，有的处理起来非常简单，有的则需高级专业人员费一番功夫才能揭露其原形。杀除文件型病毒的基本要求有两条，一是除掉病毒外壳，二是恢复原文件头。为了确定杀毒方法通常要有意让病毒传染诱饵文件，诱饵文件的长度、数据、日期时间等是已知的，并保留有原件，只要拿原件与染毒后的诱饵文件进行比较，就能知道文件在染毒前后发生了哪些变化。根据文件染毒前后发生了哪些变化根据文件染毒前后的变化可以找出：

1.染毒文件的哪一部分是病毒，即病毒附加在原文件的什么部位，杀毒的时候该从染毒文件中清除病毒。

2.病毒修改了原文件的哪些部分，被修改的部分保存在病毒的什么地方。杀毒的时候应把病毒保存的原数据存回原位置。这是指外壳型病毒在传染的时候都要修改原文件头的少量字节，被修改的原数据则保存在病毒的某个位置。

以第三章第三节的 PRGKILL 病毒为例，通过对染毒诱饵文件的分析可以看到染毒文件的第一条指令是 JMP 1003，即染毒文件修改了原文件的前三个字节，而染毒文件的 1000 到 1002 三字节的数据又恰等于原文件的前三字节，同时已经知道无毒诱饵文件的结束地址应该是 9FF 根据这些数据可以总结出杀除 PRGKILL 恶性病毒的方法是：

1.以染毒文件的第一条 JMP XXXX 指向的地址为准，倒回三个字节是病毒的起始地址，应从病毒起始地址起截断清除病毒。

2.由病毒起始地址起的三个字节保存着原文件的前三个字节数据，应移回原文件头。

第三章第三节所举染毒文件实例的杀毒处理如下：

1.染毒文件第一条指令是 JMP 1003，减 3 得病毒起始地址 1000，由

于 COM 文件加载时有长 100 的前缀，所以截断病毒后原文件的实际长度为 F00：

```
R CX
F00
```

2.把病毒保存的原文件头数据移回：

```
M 1000 1002 100
```

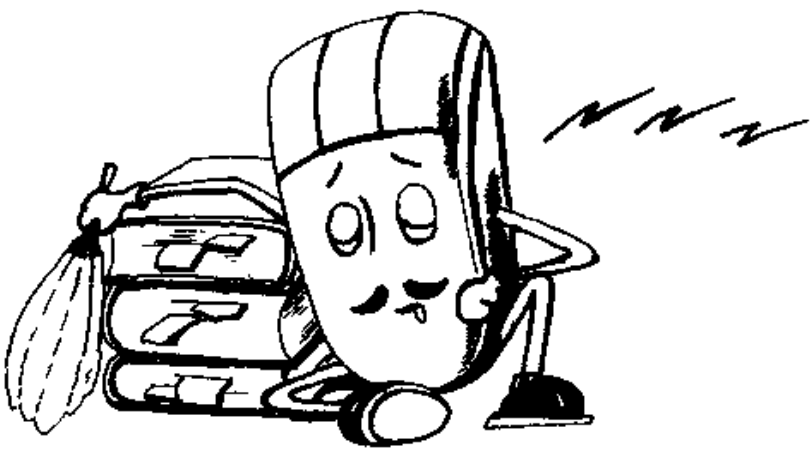
3.存储杀毒后的文件：

```
W
```

通过这样简单的操作就杀除了文件型病毒吗？对于 PRGKILL 来说确实如此。很多文件型病毒的清除过程可能要复杂得多，但其原理仍与杀除 PRGKILL 是一样的。

第五章

反病毒产品的原理与选用



随着计算机病毒的不断出现和传播，在计算机科学领域产生了一门新的学科——反病毒学。在八十年代中期，计算机病毒刚刚开始流行，种类不多，但危害很大，往往一个很简单的病毒就能在短时间内传播到世界的各个国家和地区。计算机界仓促应战，很快编制了一批早期的消病毒程序软件。消除磁盘病毒是病毒传染的逆过程。所谓病毒的传染是用一些非法的程序和数据，也就是病毒去侵占磁盘的某些部位，而消除病毒正是找出磁盘上的病毒，把它们清除出去，恢复磁盘的原状，所以消病毒软件就成了病毒的克星。早期的消病毒程序是一对一的，就是一个程序消除一种病毒。从八十年代末开始计算机病毒数量急剧膨胀，达到上千种，显然不能用上千个消毒软件去对抗上千种病毒。现今的消病毒软件已很完善，一个软件就能杀除大量病毒，并且随着新病毒的出现而不断升级。毫无疑问，消病毒软件是对抗计算机病毒，彻底解除病毒危害的有力工具。但美中不足的是消病毒软件只能检测杀除已知病毒，而对新病毒却无能为力，同时人们发现消病毒软件本身也会染上病毒。于是反病毒技术界就设想能否研制一种既能对抗新病毒，又不怕病毒感染的新型反病毒产品。后来这种反病毒硬件产品研制出来了，就是防病毒卡。防病毒卡确实能防治很多新病毒并且不怕病毒攻击，在保护用户微机信息资源安全方面起到了一定作用。不幸的是防病毒卡在实现防治新病毒的同时却失去了用户最需要的功能，防病毒卡不能消除磁盘病毒。从八十年代末到九十年代初，基本上是消病毒软件和防病毒卡并行使用，各司其职，互为补充，成为反病毒工作的主要工具。到九十年代中期，病毒数量技术继续提高，杀毒和防毒产品各自分立使用已经很难满足用户的需求，随之出现了“杀防合一”的集成化反病毒产品，把各种反病毒技术有机地组合到一起共同对计算机病毒作战，被称为第二代反病毒产品。可以肯定只要计算机病毒继续存在，反病毒技术就会继续发展。

5.1　反病毒产品的分类

在目前的计算机市场上有形形色色的反病毒产品供用户选用。然而面对丰富的市场用户往往感到困惑，不说别的，单是反病毒产品的名称就足以令人眼花缭乱：消病毒卡、防病毒卡、病毒免疫卡、安全卡、防护卡、集成化卡、可升级卡、杀病毒软件、查解病毒软件、反病毒平台、防病毒疫苗……这些反病毒产品各有什么功能，是同一类产品吗？亦或不是？

不管一种反病毒产品的名称叫什么，就其对抗病毒的作用方式，也就是所采用的反病毒技术而言，可以分为四类：

1.消除计算机病毒的产品，主要指通常所说的各种杀病毒软件，如KILL、CPAV、F-PROT等，主要功能是检测和消除磁盘病毒。

2.防治计算机病毒的产品，主要指各种各样的防病毒卡，如我国的华星免疫卡、瑞星防病毒卡、华能反病毒卡、新创卡等。也有纯软件，如DOS6系统的VSAFE.EXE。主要功能是检测内存病毒，防止病毒传染磁盘和破坏微机资源。

3.检测计算机病毒的产品，如SCAN软件。

4.集成化反病毒产品，是指把以上几种反病毒技术集成到一种产品上，使其既能杀磁盘病毒，又能防内存病毒，具有综合的反病毒能力的产品，如我国的求真可升级消病毒卡和优异病毒防治卡。

5.2　消病毒软件

消病毒软件用于消除磁盘上静态病毒，习惯上叫做杀病毒软件。常用杀毒软件有KILL、KV、DB、CPAV、F-PROT等。

计算机病毒的传染过程是首先根据某种“标志”检查要传染的部位（引导区或者可执行文件）有没有病毒，如果没有就非法地把病毒写到磁盘上。因而不难想象可以编制一种软件，其功能是根据某种特征标

志检查磁盘上的有关部位(引导区或者可执行文件)有没有病毒,如果有就采用技术手段消除磁盘上的病毒,并尽可能地恢复磁盘染毒前的原貌,这不正是"杀死"了病毒吗,因此可以说杀病毒是病毒传染的逆过程。

反病毒技术人员对大量已发现的病毒进行分析,根据每一种病毒的数据结构确定一组特征数据,作为识别该病毒的标志,同时又根据病毒的传染特性编一段消除病毒的程序,这样就构成了可以杀除大量已知病毒的杀毒软件。所以杀毒软件都有一个庞大的病毒特征数据库,记录了大量病毒的指令数据特征,或者更形象化地称之为"病毒指纹"。杀病毒软件的工作机理是对磁盘有关扇区和文件进行扫描检索,与病毒指纹一一对照,当检测到磁盘的既定部位与病毒指纹相符时,就明确报告所发现病毒的名称和染毒部位,调用相对应的杀毒程序,消除磁盘上的病毒。

消除引导型病毒的方法是根据病毒的传染特性寻找被病毒转移到其它地方的原引导区,把原引导区写回磁盘引导扇区;或者直接分析磁盘的容量类型,构造一个正确的引导区去覆盖被病毒侵占的引导扇区。消除文件型病毒则一方面要去除病毒强加在文件上的外壳,同时要恢复原文件中被修改的部分。

杀病毒技术的主要特点是:

1.计算机病毒是常驻磁盘的,通过杀病毒而"扫毒出盘",是彻底解除病毒危害的有效方法。

2.经杀病毒技术处理后的磁盘是无毒盘,使用无毒盘才能真正保证计算机的无毒安全运行,并且防止病毒通过磁盘在用户间相互传播。

3.杀病毒技术的用户界面十分友好,明确报告病毒名称和染毒部位,用户能清楚地了解计算机被病毒感染的清况。

4.与防病毒卡相比较,杀病毒技术的兼容性很好。

杀病毒软件的使用并不复杂,但要充分发挥杀毒软件的作用就应该注意:

1.杀病毒软件不象防病毒卡那样能随时监测病毒情况,什么时候

使用杀毒软件是由用户决定的，因此正确掌握杀毒软件的使用时机就显得十分重要。一方面不必要地频繁查毒杀毒既显著影响计算机的工作效率，又不利于延长驱动器的寿命；另一方面该使用杀毒软件的时候而不使用就会造成微机被病毒感染，甚至病毒发作。一般来说在微机上第一次使用外来软件前必须用杀毒软件对外来软件检查杀毒；当微机出现第四章中所提到的病毒迹象时也应及时检查是否染上病毒。

有些用户平时不在意微机异常现象，直至病毒发作后再试图用杀毒软件去"杀毒"，并因为杀毒软件处理不了被病毒破坏的硬盘而抱怨杀毒软件"无能"，这是对杀毒软件的误解。因为从理论上说杀毒软件的对抗目标是传染过程中的病毒，面不是病毒激发后的磁盘。

2.杀病毒软件本身是一种磁盘软件，如果使用不当自己也会被病毒感染。国产杀毒软件中主文件长度一般不到 100KB，由软盘加载并不费时，所以建议尽量使用软盘，软盘加写保护后可以有效地防止病毒感染。

3.杀毒软件不能识别新病毒，当出现新病毒时，低版本的杀毒软件中既没有新病毒的特征指纹，也没有相对应的杀毒程序，自然就不能识别和处理新病毒。换句话说，一种杀病毒软件要长期满足用户需求，保证其杀毒能力，就要随着新病毒的出现不断地升版升级。所以杀毒软件的合法用户要经常与软件商联系，注意所购软件的升级情况，及时升级自己的软件。

4.杀毒软件具有较强的地域性，一些著名的国外杀病毒软件虽然号称能杀除上千种病毒，但对绝大多数国内出现的病毒无效，实践证明我国消病毒产品更适合中国国情。

5.3　防病毒卡

杀病毒软件的原理决定了当一种新病毒出现时，必须由反病毒技术人员对新病毒样本进行分析，确定特征码和编制相应的杀毒程序，通过对老版本杀毒软件的升级，才能杀除新病毒。所以杀毒软件对抗新

病毒或多或少总有一点滞后性，于是90年代初我国计算机工作者发明了一种能在一定程度上对抗新病毒的反病毒产品——防病毒卡。

防病毒卡的作用机理是监视微机内存中动态病毒的行为公性，公性的概念比较抽象，我们通过一个比喻来形象地说明防病毒卡与杀病毒软件在检测病毒方面的差异。大家知道近年来国际足球比赛中不良球迷闹事已经成为一大公害，特别在欧州每遇大赛警方都如临大敌。为防止不良球迷闹事，警方采取两套方案，一是记录足球流氓的个人特征，如拍照片提取指纹，分发到各有关单位。以照片指纹为依据，不让有前科的足球流氓人境和进入赛场。第二方案是在赛场内部署警力，监视比赛现场情况，发现球迷闹事予以制止。

如果把微机比作赛场，那么上面的例子在一定程度上说明了杀病毒和防病毒的作用原理。杀病毒针对的是病毒个性，即磁盘上的静态病毒，通过杀除外来磁盘上的病毒而根本不让病毒进入微机硬盘。防病毒卡不能杀除外来病毒，当用户在未察觉情况下把带毒的外来软件拷贝到硬盘上时，防病毒卡对硬盘上的病毒是无能为力的。但带毒软件运行时病毒进入微机内存，防病毒卡会监视内存病毒的行为公性。比如说大部分引导型病毒都占据常规内存高端、修改0413存储器和INT13中断。因此防病毒卡监视到微机内存中发生上述现象，就可以认为内存中有一个引导型病毒正在活动。所谓防病毒是通过分析大量已知病毒，根据它们的机理、传染和破坏行为的共同规律特性分成若干类群体，在此基础上编制成监视病毒共性的防病毒程序，固化到E-PROM存储器中做成防病毒卡。当防病毒卡监测到病毒行为时，就认为内存中有病毒在活动发出报警，采取一些措施尽量中止内存病毒的活动，防止病毒传染和破坏，有的卡叫“除去内存病毒”；又有的叫“过滤内存病毒”等。在一些情况下，防病毒卡监视到磁盘分区表、DOS引导区、FAT表以及可执行文件等的重要部位有可能被修改，但又不能肯定是病毒所为，就采用疑问式报警提醒用户注意，由用户判断合法性，回答YES或者NO表示同意或者不同意修改。

防病毒实质是对微机操作系统的一种监控补充，对于DOS系统病

毒,监控的主要对象是有关软中断调用。例如监测 INT13,当发现入口处寄存器 AH、CX、DX 的值分别为 03、0001 和 0080 时,表明硬盘主引导区将被改写,从而发出相应警告。对硬盘引导区的合法修改仅限于硬盘分区、格式化等极少数操作,也只有专业人员才进行这些操作,所以很容易与病毒的非法修改相区分。可以说保护磁盘引导区是防病毒技术成功运用的一种例子。对 DOS 调用 INT21 的监控则要复杂得多,作为开放系统,DOS 允许修改 INT21 中断地址,因此单纯的中断地址向量变化不能判为病毒,而必须再附加至少一个条件,例如对文件的非法修改才能认定为病毒。

防病毒卡对病毒的检测不依赖病毒的个性特征,而是根据已知病毒群体的共同行为,所以能够防治新出现的,而又没有原理性发展的新病毒。仍以引导型病毒为例,如果新病毒在占用内存、传染途径等方面找不到新路子,仍然占据常规内存高端,依旧修改 INT13,则不论病毒的磁盘记录如何变化,从而形成多种新病毒,但它们进入内存后只不过是"故技重演",就都能被防病毒卡检测出来。所以防病毒卡的主要特点是能够防治没有原理性突破的新病毒。

但在另一方面不能把防病毒卡的功能无限扩大,因为防病毒卡所能预测的病毒公性同样是设计人员对已知病毒的分析得来的。如果新病毒采用了新的机理,从而产生防病毒卡检测不到的传染破坏行为,防病毒卡就会"漏报"病毒。在防病毒卡发展史中最著名的漏报事件是 DIR-II 病毒,90 年代初设计的防病毒卡主要靠监视 INT21 中断来判别病毒,但 92 年出现的 DIR-II 病毒并不修改 INT21 就达到传染目的,所以当时的防病毒卡没能防得住 DIR-II 病毒。表现为病毒已经进入内存并传染文件,而防病毒卡却无反应。类似的情况后来也发生过,比如 94 年发现的 ANTISCAN 和 BACKFORM 病毒都使一部分防病毒卡失效。90 年代前期曾经有防病毒卡"可防一切未知病毒"说法,在理论上就站不住脚,因为如果真的有"可防一切病毒"的产品,那么计算机病毒问题不是一劳永逸地解决了吗?

防病毒卡作为一种扩展微机功能的硬件产品,具有一些很突出的

"硬"特点。在微机上电过程中,扩展硬卡先于磁盘系统启动,使反病毒系统优先于一切磁盘病毒完成初始化,既能有效地拦截开机过程中的引导型病毒,又能预先建立防治文件型病毒的体系。硬卡的工作具有实时性,从开机上电直到关机,微机系统始终处于硬卡的监视下,而且占用微机 RAM 内存。硬卡本身是完全免疫的,病毒不可能攻击改变硬卡上的反病毒系统。这些"硬"特点是磁盘软件不可能实现或者很难实现的。

防病毒卡的主要不足是只防病毒不杀病毒,防病毒卡报告的清除病毒是指内存中的动态病毒,对磁盘上的静态病毒则无能为力。当使用染毒磁盘时,防病毒卡即使能发现报警,磁盘上的病毒也是"安然无恙"。而用户的要求恰恰是消除磁盘病毒,所以可以说没有杀毒功能的纯防病毒卡不能构成完整的反病毒系统。另外防病毒卡的工作原理是先让病毒进入微机内存,再根据其行为进行判定,所以造成微机"带毒运行",对微机是不安全的。

防病毒卡还存在"误报"问题,即在没有病毒情况下防病毒卡判断为有病毒活动。误报的责任有时不在防病毒卡一方,有些软件采用不规范编程,过于复杂的加密,甚至不惜用"定时炸弹"来"保护版权",就有可能被防毒卡判断为病毒。值得注意的是防病毒卡的"漏报"病毒和"误报"病毒往往是相互关联的,防病毒卡对病毒监视得严一些,其"漏报"就较少,可以较好地预防新病毒,但它的"误报"可能相对略高;反之,防病毒卡对病毒监视得松一些,其"误报"就较少,但"漏报"病毒的可能性高一点。所以防病毒卡的技术指标较难度量,不同的用户根据自己的体验往往对同一种防病毒卡作出不同的评定。

5.4 集成化反病毒产品

杀病毒软件和防病毒卡都是对抗计算机病毒的有力武器,但检测病毒的原理、对病毒的处理结果及其所依附的载体均不相同,表现出较大的功能差异。杀毒软件可以杀除大量已知病毒,却不能随时抵御新

病毒的攻击。特别如果杀毒软件更新不及时，以至于新病毒激发，会给微机造成很大危害。而且磁盘软件的物理可靠性低于硬卡。防病毒卡可以预防新病毒，在微机运行过程中随时保护微机的重要资源，不怕病毒攻击，其根本的弱点是不能杀除磁盘病毒致使微机带毒运行。

通过分析对比，很容易发现"杀病毒软件"和"防病毒卡"的功能特点在很多方面都是相左的：它们都具有对方无法取代的优点，又有自身难以克服的不足。如果研制出一种新的反病毒产品，它能融"杀"和"防"病毒于一体，扬长避短，发挥两种技术各自的优势，抵消其各自的缺点，则新产品的反病毒能力将大大增强。计算机专家称集预防、检测和消除三大功能于一体的反病毒产品为"集成化"产品，集成化是反病毒技术发展的必然趋势。

集成化反病毒产品有两类，一类是软件集成化。常用的 CPAV 就是一个集成化的反病毒软件包，这个软件包中的 CPAV.EXE 用于杀病毒，VSAFE.EXE 用于防病毒。但是纯软件防病毒的特性远不如防病毒卡，特别在内存使用方面，硬卡则可做到完全不占用户内存，而防病毒软件要占用数十 K 用户内存，所以防病毒软件很少使用。

集成化产品的另一方向是反病毒硬卡，硬卡不仅用于防内存病毒，而且能杀磁盘病毒。硬卡杀病毒所遇到的最大技术障碍是升级问题。通常各种计算机硬卡需要升级时要由用户把卡送回（或寄回）原生产销售单位，由销售商进行升级处理。这种升级方式显然不适用于反病毒卡，经济上每次升级用户都要支出姑且不论，单以时效性考虑，杀病毒技术原则上要求当出现新病毒时要随时升级。据 90 年代前期统计，国内平均每个月出现两、三种新病毒，不难想象如果采用传统的销售商升级方式，本地用户的麻烦自不待言，外地用户的升级就几乎成为一句空话，可见升级难是阻碍硬卡集成化的主要障碍。

我国科技工作者经过长期研究，在世界上率先解决了硬卡升级的技术难题，研制成功可升级的集成反病毒卡，代表产品有"求真可升级消病毒卡"和"优异病毒防治卡"。这两种集成反病毒卡都是以杀磁盘静态病毒为主，防内存动态病毒为辅，杀防合一构成完整的反病毒体

系，并且都具有硬卡自升级功能。

集成反病毒卡的杀毒原理与杀病毒软件相同，都能准确地检测和消除磁盘上的静态计算机病毒，但两者的工作时间状态不同。杀毒软件由用户控制使用，即在用户认为有必要时中止其它软件运行，用杀毒软件杀毒；反之当其它软件工作时，杀毒软件则不起作用，所以正确把握杀毒软件的使用时机是很重要的。集成反病毒卡则具有"实时"杀毒功能，集成卡在不需要用户干预情况下自动监视将要进入内存的磁盘软件，发现病毒即予报警杀除。比如当用户输入可执行文件名并回车的时候，集成化反病毒卡会监视到微机将要加载执行一个软件，立即检查该文件是否含有病毒，如果检查出病毒随即杀除磁盘文件中的病毒，然后加载杀毒后的无毒文件。当集成化卡遇到新病毒的时候也会出现一时不能杀除的情况，这时集成卡将起防病毒卡的作用，报告发现了未知名称的新病毒。

集成反病毒卡的防毒原理与防病毒卡相同，都是监测内存动态病毒和保护微机信息资源，但两者防治的对象不同。防病毒卡不能杀毒，其所防治的对象是所有病毒，即不论是早就出现的老病毒，还是新流行的病毒，防病毒卡都是让病毒进入微机内存后再去检测防治；集成反病毒卡则不然，对于大量已知病毒，集成卡根本不让其进入内存就予以杀除，所以集成卡防治的对象只是新出现的病毒。

求真卡和优异卡都是可由用户自己（而不是由销售商）通过简单的操作就能升级的"可升级卡"。当发现新病毒后由研制单位以清单或磁盘方式向用户提供一个小程序，用户只要在自己的微机上运行这个小程序，就能使集成化卡升级杀除新病毒。硬卡升级的最大得益者是用户，免除了用户的后顾之忧。求真卡的升级程序在〈中国计算机报〉、〈软件报〉上公开发表，所以用户只要订阅报纸就能免费获得升级程序。

综上所述，集成化卡对抗计算机病毒的策略是：

1. 在微机运行过程中实时监测磁盘引导区和可执行文件，发现病毒立即杀除，保证磁盘和微机无毒运行。

2. 当新病毒出现时，防病毒系统予以报警，保护微机重要资源，即

起防病毒卡的作用。

3.通过简单的自升级提高卡的功能，包括杀除新病毒，使卡的杀毒种类越来越多。

与防病毒卡比较，集成化反病毒卡在保留防病毒功能的基础上实现了重要的杀磁盘病毒功能，并且可以由用户自行升级，其性能价格比有了明显的提高，被称为第二代反病毒卡，将逐步取代第一代防病毒卡。

集成化卡还有一个特点是采用兆位级大容量固态存储器，通常是防病毒卡容量的十几倍到几十倍。比如优异卡为 128KB，求真卡有 128KB、256KB 和 512KB 三种，除了支持反病毒系统外，还有足够的存储空间可固化其它系统软件，比如国家标准汉字库和一些常用的驻留系统，使卡的集成度进一步提高，由专用的反病毒卡向多功能卡发展。

目前世界上唯有我国能够生产可升级集成化反病毒卡，这说明我国的反病毒软硬件技术居于世界前列。

5.5　怎样选用反病毒产品

在品类众多的反病毒软硬件产品中怎样以有限支出获得高性能产品是广大用户十分关心的问题，一般来说在选购反病毒产品的时候建议注意以下方面：

1.明确产品的功能特性，如前所述反病毒产品的功能分为防病毒、杀病毒和集成化几种，单凭产品名称难以准确表达产品特性，所以一定要向销售商问清楚。

2.根据被保护对象选用合适的产品。家庭微机具有硬盘容量大，软件交流频繁、备份少等特点，又是家庭中的一个“大件”，宜选择杀防结合方式来反病毒，可选杀毒软件与防病毒卡搭配使用，也可选集成化反病毒卡。微机较多的机关单位可在重要部位微机上安装反病毒硬卡，而其它微机用杀毒软件。

3.价格因素，目前国产正版杀毒软件的价格从 200 元到 250 元；名

牌防病毒卡从 430 元到 495 元;具有杀防功能并且可升级的集成化反病毒卡从 496 到 550 元,这些都是可供参考的含税零售价。如果发现所选购产品价格明显偏高就要了解是否增加了其它功能,增加的功能对自己是否有用。如果价格明显偏低,并不一定是好事,比如可能是没有任何售后服务的侵权盗版产品;也可能是积压淘汰产品。外国反病毒软件包零售价格 100 多美元,批量可降到数十美元,但国内较少见到正版软件。

4.获得确实的售后服务保证,特别是产品升级保证。大家知道任何计算机产品都有升级换代问题,而反病毒产品对升级尤为敏感。一种反病毒产品不论其出售时如何先进,如果不能根据病毒的发展适时升级,抵御不了新病毒则随时会成为没有用的"废品"。升级有两种方式,一种是产品本身没有升级功能,升级工作完全由生产或销售单位完成,但可能互相推脱。比如有的销售单位不管升级,要用户找生产单位,其可行性就很差,特别当用户与生产单位不在同一地区时,产品升级将十分困难。同时由于用户不掌握升级主动权所以要问清楚厂商升级时是否收费及收费标准。另一种升级方式是产品本身具有升级功能,而升级程序数据由设计单位提供,途径有通过媒体公开发表,磁盘和远程通讯传送等,一般是不收费的。应该清楚不论是杀毒产品还是防毒产品都有升级问题,有些产品长期不升级或者产品已经升级而用户不予注意,对微机来说都是危险的。

5.使用正版产品。反病毒是关系用户微机安全的大事,应注意选用正版产品才能获得长期的售后服务和升级保证。社会上有一些盗版软硬件在流行,如 KILL.EXE 正版达到 71 版时市场上竟有 77 和 80 版出售。盗版软件多半是修改低版本软件的版本号,无中生有地冒充高版本软件出售欺骗用户。使用盗版软件将给用户造成虚假的安全感,危害至深。当微机有染毒征兆的时候,使用假冒的高版本的软件检查可能根本查不出病毒,而用户却放松了警惕,病毒一旦激发后果难料。所以可以说盗版反病毒产品是计算机病毒的"帮凶",与病毒合起伙来欺骗用户。

6.有些用户在选购杀毒产品的时候比较关注可杀"多少种"病毒。目前国际上还没有关于病毒命名的统一标准和权威机构。出于商业等因素,不同厂商对病毒的划分会有很大差别。以黑色星期五病毒为例,有的厂商按它的几十个变种统计,有的厂商则只算一种病毒,比较之下当然是后者比较严谨。但在统计数字上仅这一个病毒前者就要比后者"多"出几十种。据报道国外一些可杀数千种病毒的软件对国内出现的很多病毒检测不出来,所以我国用户应注重杀毒软件对本土病毒的检测杀除情况,而不拘泥于厂商宣称的指标。

7.注意产品包装,包装粗糙的产品往往是小厂临时生产的,没有可靠的技术服务保障。

8.在选用硬卡时应注意有无开机关卡功能,因为防病毒卡总有少量误报问题,如果没有关卡功能则当卡误判病毒时必须拔掉卡才能运行用户软件,反复拔卡和插卡是不符合硬件操作规程的。

9.反病毒产品与其它产品一样也要受市场经济的影响,近年来国内外先后有一些比较著名的厂商停止反病毒产品的研究。或改变方向搞其它"利润更大"的产品,或被其它企业兼并,所以在选购的时候要注意厂商在反病毒领域的发展前景。

几种反病毒产品的特性表

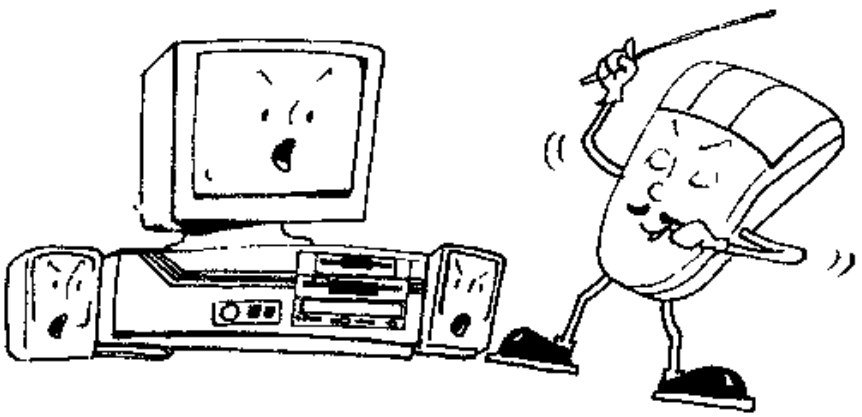
	杀病毒软件	防病毒卡	杀防合一的集成化卡
对抗病毒的效果	杀除磁盘已知病毒,通过升级杀新病毒	防治已知机理新老病毒,不能杀磁盘病毒	杀除磁盘已知病毒和防治已知机理新病毒,通过升级杀新病毒
微机安全性	对可杀病毒保证微机安全,不可杀的新病毒无安全性	对可防的病毒具有一定安全性,但不能绝对化	对可杀病毒保证微机安全,对可防的病毒具有一定安全性,但不能绝对化
报警时的用户界面	明确界面友好	比较模糊	杀毒时明确界面友好防新病毒时比较模糊

续表

	杀病毒软件	防病毒卡	杀防合一的集成化卡
工作实时性	静态查毒杀毒不能随时监控病毒	动态防病毒，可随时监控病毒	动态杀毒和防毒，可随时监控病毒
产品安全性	可能感染病毒	不会感染病毒	不会感染病毒
产品可靠性	可能物理损伤	坚固	坚固
兼容性	很好	存在兼容问题	杀毒模式很好，防毒模式存在兼容问题
升级性	可升级	无自升级功能	可升级

第六章

典型反病毒产品的应用



6.1 KILL 计算机病毒清除工具

KILL 计算机病毒清除工具是中国金辰安全技术公司编制的消病毒软件，有 5 英寸和 3 英寸软盘两种产品可供选用，两种软盘都是 DOS3.31 系统引导盘。KILL 是加密的，可以在产品软盘上使用，也可以把文件拷到硬盘上用，但在硬盘上使用时，仍然要求把产品软盘插入 A 或者 B 驱动器。KILL 的使用比较简单，只要键入命令：

KILL [盘符：[\ 子目录名 \ ][文件名]] (中括号内为选项，可以省略，下同)屏幕上即显示功能菜单，可以用左右箭头键选择功能：

SCAN	CLEAN	RESIDENT	TOOLS	DRIVE C	QUIT
Scanning memory for virus Found virus in memory, *REBOOT* system !!!				Found viruses : 0 Checked files : 0 Cleaned files : 0	
Kill V 7 5 . 0 3 Copyright (c) by The Ministry of Public Security PRC 9 5 . 1 1 . 8					

图 6-1 KILL 计算机病毒清除工具菜单

DRIVE 选择盘符、子目录及文件名。选择时可以不带文件名只选盘符及子目录。如果带文件名的话，则必须是一个确定的文件名，而不能使用通配符。

SCAN 检查病毒，包括三个方面：

1.检查内存病毒，当发现内存病毒时说明在使用 KILL.EXE 文件前已经运行了带病毒的其它软件，因为带毒运行是不安全的，所以 KILL 将要求重新开机。

2.检查指定盘的引导区病毒。

3.检查指定盘及子目录下的文件,KILL 不但检查 COM 和 EXE 文件,而且对各种扩展名的文件都进行查毒。这样处理的好处是查毒更严密一些,但检查大容量盘时速度显得慢一些。

CLEAN　清除病毒,这是在 SACN 查到病毒的情况下杀除磁盘上的病毒。

QUIT　中止 KILL 运行,退回到 DOS。

KILL 窗口菜单中的 RESIDENT 和 TOOLS 功能是给专业人员用的,暂时还没有配上。

在检查和清除病毒过程中,窗口左边显示文件名和病毒名,窗口右边显示所发现的病毒种类数、检查以及杀毒的文件数。

KILL 软盘上还有名为 VLIST.TXT 的病毒列表文件,可以用 TYPE 命令显示或打印,也可以用 WS 等编辑软件观察。

6.2　反病毒软件包 CPAV

CPAV 是美国 Central Point 公司的反病毒软件包,全称是 Central PointAnti-Virus。在 DOS6 系统中引入了 CPAV,主文件名是 MSAV.EXE,使用方法与 CPAV 相同,所以对 CPAV 的介绍也适用于 MSAV。CPAV 软件包的目录如下:

AUDIT	CPS	1,751	01-08-94	3:42p
AVINST	HLP	48,300	06-01-93	2:00p
BOOTSAFE	EXE	32,065	06-01-93	2:00p
CPAV	EXE	551,856	06-01-93	2:00p
CPAV	GRP	2,531	06-01-93	2:00p
CPAV	HLP	56,111	06-01-93	2:00p
CPAV	ICO	766	06-01-93	2:00p
CPAV	BAK	866	01-24-94	7:56a
CPAV	PIF	545	06-01-93	2:00p

CPB	OVL	2,956	06-01-93	2:00p
CPSHELP	OVL	29,828	06-01-93	2:00p
CPSMM	BIN	2,993	06-01-93	2:00p
EXCEPT	CPS	804	06-01-93	2:00p
README	TXT	6,929	07-20-92	9:08a
SMARTCHK	CPS	1,200	06-01-93	2:00p
SMARTSIG	CPS	12,077	06-01-93	2:00p
VIRULIST	CPS	44,928	06-01-93	2:00p
VSAFE	EXE	74,145	06-01-93	2:00p
VSAFE	SYS	72,176	06-01-93	2:00p
VWATCH	COM	47,403	06-01-93	2:00p
VWATCH	SYS	48,272	06-01-93	2:00p
CPAV	INI	866	09-12-95	5:06a
VIRUS	DAT	10,517	08-02-93	9:00a
REPORTS	〈DIR〉		08-02-95	3:53p

27 file(s) 1,057,025 bytes
2,437,120 bytes free

一、杀病毒软件 CPAV.EXE

CPAV.EXE 的主要功能是检测消除磁盘病毒，CPAV 为全窗口下拉式菜单操作，支持鼠标操作，可以用字母键、箭头键和鼠标三种方式选择功能，用户界面很友好，反病毒功能比较完善。用 CPAV 命令进入后用 F8 键选择窗口方式，全屏幕窗口如图 6-2，可用 F2 键选择驱动器(也可在 DOS 提示符下用 CPAV 盘符命令直接选择驱动器)。图 6-2 左下方框是选定磁盘的目录树，右下方框是部分文件名。屏幕第 2 行 Scan、Options、Configure 和 Help 为功能选项，击词头大写字母键进入，例如击 S 键进入 SCAN。

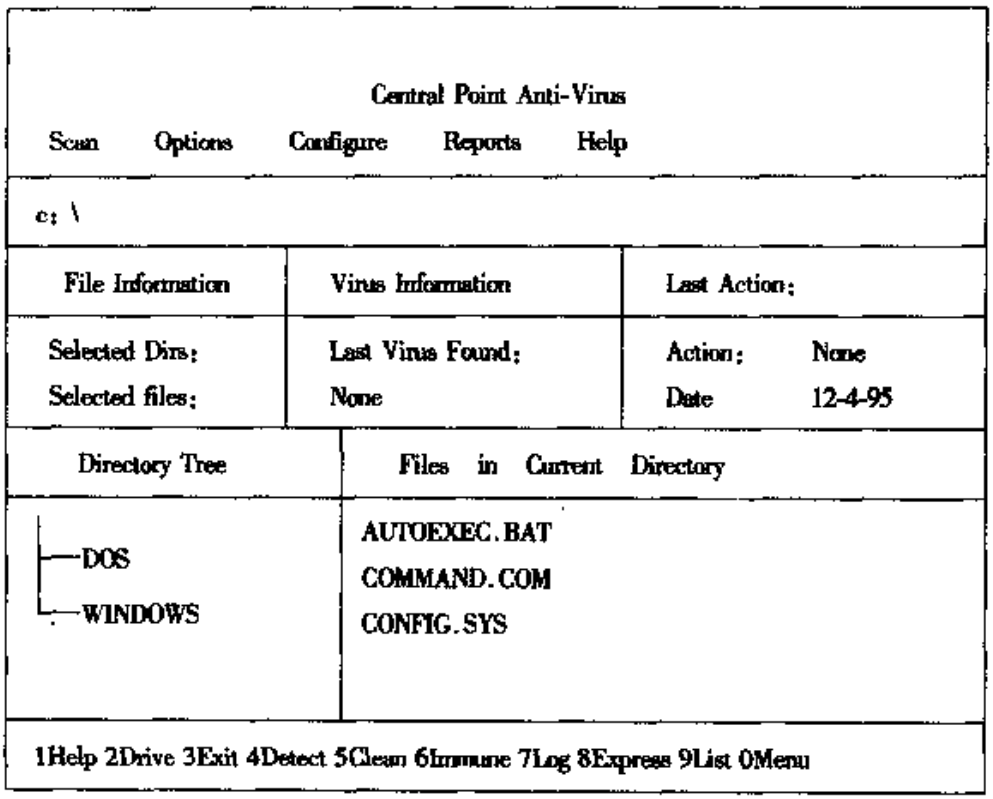


图 6-2　CPAV 主菜单

1. Scan 检测和杀除病毒

在图 6-1 状态下击 S 键进入 CPAV 的主功能 Scan，屏幕显示 Scan 次级菜单如图 6-3，可移动光标分别进入 9 项功能，主要功能介绍如下：

(1)Detect　检测病毒

对指定的磁盘进行扫描检测病毒，发现病毒时显示如图 6-4。

图 6-4 指出在 XCOPY.EXE 文件中发现 Omicron 病毒(又称 FLIP、2153)，有 4 种选项处理方式：

Clean　消除当前文件中的病毒；

Continue　不处理当前文件，继续向下运行；

Stop　停止扫描查毒，回到图 6-1；

Delete　删除当前文件。

Detect
Detect & Clean
Immunize
Remove Immunization

Delete Checklist files

Virus List
Update Virus List
Activity Log

Exit

图 6-3 SCAN 菜单

Virus Found

Omicron was found in: XCOPY.EXE

Clean Continue Stop Delete

图 6-4 CPAV 发现病毒的报告

CPAV 在查毒过程中有时会显示发现病毒代码 Viral code B 或 Viral code F,分别表示引导型和文件型病毒。选杀毒 Clean 后屏幕上显示一大段英文信息,大意是 CP 公司还没有这种病毒的样本,请用户把病毒样本寄到公司,以便分析后提供杀毒程序。这是 CPAV 所做的一种模糊判断,究竟是不是病毒,以及如果真是病毒又怎样杀除都需要反病毒部门进一步分析后才能确定。

Detect 查毒完成后屏幕上显示一个报告,告知用户所检查的驱动

器数、文件数、发现和杀除病毒的数目以及查毒所用时间。

(2)Detect & Clean 检测和杀除病毒

其过程与 Detect 相同,只是在发现病毒后不显示图 6-4,而立即杀除病毒。

(3)Immunize 免疫

免疫功能,给可执行文件增加免疫"外壳",外壳中记录了被免疫文件的有关原始数据。在运行免疫文件时 CPAV 增加的免疫外壳将检查文件本身是否变化,如果文件发生了变化(可能是感染了病毒),屏幕上会提示:

```
Self interrity Check warning File was changed!
Choose an option
[R] Self Reconstruction
[C] Continue execution
[E] Exit DOS
```

图 6-5　免疫文件变化的报告

图 6-5 表示免疫文件发生了变化,中括号内给出三个选项:

[R]自恢复功能,放弃已发生的变化,把文件恢复到变化前,即免疫时的状态;

[C]不理会已发生的变化,继续运行文件,一般用户慎用此功能;

[E]停止运行当前文件,退回到 DOS 状态下。

关于 Immunize 的使用应注意以下三点:

(A)Immunize 的功能是当文件变化后予以报告并提供了恢复文件的可能,不是完全阻止文件的变化(技术上也不允许),所以尽管 Immunize 的含义是"免疫",但不能理解为经 Immunize 处理后的文件可以免受病毒感染。

(B)有一些文件不能 Immunize,特别是 CONFIG.SYS 文件要调用的可执行文件。如果 Immunize 后微机不能启动,多半是对 CONFIG.SYS

用到的文件 Immunize 的结果，应找出相关文件去掉其免疫外壳。

(C)经 Immunize 处理的文件长度要增加，即外壳的长度，CPAV2.0 免疫外壳长 779 字节。因为文件长度增加，一些用户误当做"病毒"。特别是把经 CPAV 免疫后的文件拷贝到另一台未安装 CPAV 软件包的微机上使用会带来一些麻烦。

(4)Remove Immunization 除去免疫

除去第(3)项 Immune 功能所加的免疫外壳。如上所述 Immune 不是一个万全的反病毒功能，而且有些文件 Immune 后会出现运行异常，可用本功能除去其免疫外壳。

(5)Virus List 病毒列表

列出CPAV所能检测和杀除的病毒清单，如图6-6。清单中给出病毒名称、类型和长度。可以用上下箭头键上拉和下拉清单，如果觉得

Virus List			
Name	Type	Size	#
Disk Killer	Boot	3072	2
Ogre			
Disk Killer 2	Boot	3072	1
Dismembe	File	288	2
DIR	File	691	1
DIR 2	File	1024	1
DIR 2-A	File	1024	1
DM	File	400	1
Doctor	Boot	4608	1
Dodo	File	408	2
Dodo Pig	File	407	1
		Find	Next
Info	Print	OK	

图 6-6　CPAV 病毒列表

速度慢请注意图 6-6 下方有光标闪动，在光标处打入字母会立即切换清单。比如要找 Casper 病毒，则击 C 键清单中立即显示以字母 C 打头的病毒，当然可以继续击 A、S 等键以快速找到 Casper。图 6-6 下方有 Info 功能，可击 ALT-I 键进入，显示病毒的详细特性。

(6)Exit 退出

2.Option 设置功能选项

在图 6-1 状态下击 O 键进入 Option 菜单，项目较多，每一项左侧有一个正方形符号"□"，用箭头键把光标移到所选项上，反复击回车键，"□"符号内出现"√"表示该项目有效；"□"符号内为空白则该项目无效。主要项目介绍如下：

(1)Verify Interrity 比较检验

在 SACN 扫描磁盘过程中与 CPAV 产生的 SMARTCHK.CPS 文件进行比较，SMARTCHK.CPS 文件保存着上一次使用 CPAV 时磁盘文件的检查记录，如果本次扫描的结果与上一次不同，则显示变化值提醒用户注意。

(2)Create New Smartchecks 建立要点文件

在 SCAN 扫描过程中为每个子目录建立 SMARTCHK.CPS 文件，SMARTCHK.CPS 文件中保存本目录下每个可执行文件的校验和、长度、属性、最后修改日期等重要信息，为上一项 Verify Interrity 功能提供比较依据。

(3)Scan Compressed files 检查压缩文件

选择此功能可以检查由 ARJ、LHA 等打包软件所产生的压缩软件包中的病毒，检查的时候需要对压缩包解压缩，所以整个扫描速度较慢。如果放弃此项功能，当然就不检查压缩包，但扫描速度大大加快。经实验检查 486DX 微机的 100M 逻辑盘，检查压缩包费时 8 分多钟，而不检查压缩包仅 1 分 40 秒，所以用户要根据实际情况决定是否选用此功能。CPAV 对把有些非压缩的可执行文件当成压缩文件来处理，这是 CPAV 的一个缺陷。

CPAV 的功能项目很多，以上介绍的只是部分主要功能，更详细的

使用方法可以在 6-1 菜单下击 H 键进入帮助状态逐一浏览各项说明。

二、防病毒软件 VSAFE.EXE

VSAFE.EXE 是 CPAV 软件包中的一个防病毒软件，并被 DOS6 系统选用做为外部命令。VSAFE 是驻留软件，执行 VSAFE 后屏幕上显示图 6-7。图 6-7 提供了版本版权信息，下面 4 行是内存占用情况。图6-7 还告诉用户呼出 VSAFE 选单的热键(Hotkey)是 Alt + V，即先按住 Alt 不放再按下 V 键将呼出 VSAFE 的功能选择菜单，如图 6-8 所示。

```
VSafe (tm)
Version 2.0
Copyright (c) 1991-1993
Central Point Software, Inc.
Hotkey: 〈Alt〉〈V〉

VSafe successfully installed...
Vsafe is using 24K of Convertinal memory
              0K of Upper memory (UMB's)
             24K of XMS memory
              0K of EMS memory
```

图 6-7　驻留 VSAFE 的屏幕显示

图 6-8 标号 1 到 8 是 VSAFE 的 8 项功能，当右边 ON 为选通状态，“ ”表示该项功能选通有效，空白表示未选通。选择方式是反复击数字键，例如图示状态第 7 项“Protect FD boot sector”即软盘引导区保护为选通，现要撤消此项保护可击一下对应的数字键 7，ON 选通栏变为空白；如果又要恢复软盘保护可再击 7 键。8 项功能作用如下：

(1) HD Low level format	硬盘低级格式化保护
(2) Resident	软件驻留内存保护
(3) General write protect	一般写保护
(4) Check executable files	检测文件型病毒

(5) Boot sector viruses　　检测引导型病毒
(6) Protect HD boot sector　　硬盘引导区保护
(7) Protect FD boot sector　　软盘引导区保护
(8) Protect executable files　　可执行文件保护

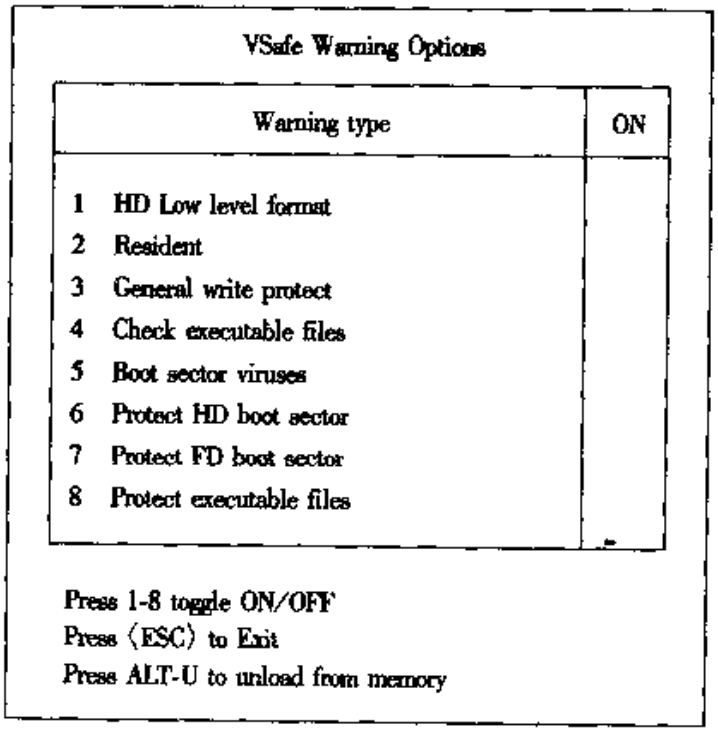


图 6-8　热键 Alt + V 呼出的 VSAFE 功能选单

这些项目中(1)(6)(7)(8)的作用比较明显，是保护磁盘重要部位不被非法修改。当被保护对象被修改时屏幕上会出现 VSAFE 报警信息，并提供停止(Stop)、继续(Continue)和重新启动微机(Boot)三个选项供用户选择。如果用户确认是合法改写可选 Continue，否则选 Stop 或 Boot。(4)(5)两项分别检测已知文件型和引导型病毒，如果发现病毒将报警并可调 CPAV 杀毒，但实测杀毒效果不好，建议慎用。(2)(3)两项功能与正常软件冲突较大，一般很少使用。

尽管 VSAFE 被称为防病毒软件，但它能有效提供的主要是一些保护措施，不象我国研制的防病毒卡那样可以防治新病毒。同时在图 6-6 中可注意到 VSAFE 占用的内存是比较可观的，当 VSAFE 全部驻留常规

内存时要占去40多K字节，就目前微机应用况而言是完全不允许的；如果分别驻留到常规内存和扩展(或扩充)内存，则与其它软件冲突的机率又增大。当VSAFE与其它软件冲突时可以用热键Alt+U中止VSAFE工作，释放它所占的内存。

6.3 SCAN和CLEAN软件

英文SCAN是扫描检测的意思，CLEAN是清除，反病毒软件中以这两个英文词作文件名的不止一家，其中以美国McAFee公司的产品比较有名，所以现在一般说SCAN就是指McAFee公司的反病毒软件包。SACN.EXE用于检测病毒，CLEAN.EXE用于消除病毒，SCAN软件包中的文件目录如下：

```
Volume in drive D has no label
Volume Serial Number is 1C22-2F49
Directory of D:\SCAN

.            〈DIR〉          09-04-95   1:26a
..           〈DIR〉          09-04-95   1:26a
AGENTS   TXT      31,481 04-04-95   11:42a
CLEAN    DAT      64,716 04-04-95   11:42a
COMPUSER TXT       6,252 04-04-95   11:42a
FILENAME TXT       1,956 04-04-95   11:42a
FILE-ID  DIZ         147 04-04-95   11:42a
LICENSE  TXT      16,483 04-04-95   11:42a
NAMES    DAT     163,083 04-04-95   11:42a
PACKING  LST       1,145 04-04-95   11:42a
README   1ST       1,526 04-04-95   11:42a
REGISTER TXT       9,857 04-04-95   11:42a
```

```
SCAN        DAT      162,480 04-04-95   11:43a
SCAN        EXE       97,839 04-04-95   11:43a
VALIDATE    EXE       15,958 04-04-95   11:43a
VALIDATE    TXT        3,560 04-04-95   11:43a
VIRUSCAN    TXT      240,479 04-04-95   11:43a
CHKVSHLD    EXE       18,945 04-04-95   11:43a
VSHIELD     DAT      192,816 09-04-95    1:27a
VSHINST     EXE       44,110 04-04-95   11:44a
VSHLDCRC    EXE       45,091 04-04-95   11:44a
VSHLDWIN    EXE       29,394 04-04-95   11:44a
VSHEMU      EXE       30,876 04-04-95   11:43a
VSHIELD     EXE      206,697 04-04-95   11:43a
        24 file(s)     1,384,891 bytes
                      31,035,392 bytes free
```

SCAN 采用了传统的 DOS 界面，与 WINDOWS 式的华丽窗口界面比较，DOS 界面被认为是“冷冰冰”的，但简单实用。用 SCAN 查毒时要使用带参数的命令，格式是：

SCAN [object1] [object2...] [option1] [option2...]

其中[object1] [object2...]为要检测的磁盘盘符、路径及文件名(可以用通配符)，中括号[ ]表示该项可以省略(下同)。比如检测 A 盘和 C 盘根目录及 DOS 子目录下的病毒可以使用命令：

SCAN A: C:\ C:\DOS

[option1] [option2...]代表功能选项，用斜杠符“/”加字母表示。主要功能选项有：

/ADL	Scan all local drives	检测所有本地驱动器
/ADN	Scan all network drives	检测所有网络驱动器
/ALL	Scan all files.	检测所有文件

/CLEAN	Clean viruses from infected files and system areas.	在检测到病毒的时候消除病毒
/DEL	Delete infected files	删除染毒的文件
/FAST	Faster scanning (may miss some infections)	快速检测但可能漏掉某些染毒文件
/LOG	Save date and time of the current scan to the log file.	把当前检测的数据和时间保存到 LOG 文件
/MOVE〈directory〉	Move infected files into 〈directory〉, preserving path.	把染毒文件移到指定的子目录中保存
/NOCOMP	Do not scan compressed files internally	不检测压缩文件
/NOMEM	Do not scan memory for viruses	不检测内存病毒,在一些286、386 微机上 SACN 检测内存病毒的速度相当慢,当已经确认内存中没有病毒的时候可用此功能加快检测速度
/PAUSE	Pause at end of each screen page	屏幕暂停,SCAN 在检测过程中如果显示的信息较多将发生屏幕翻屏,造成先显示的信息"丢失",此功能使在显示满一屏时暂停,以便观察信息。
/VIRLIST	Display virus list	病毒列表

以上是 SCAN 的主要选项功能,要了解 SACN 的全部选项可以直接

键入不带参数的 SCAN 命令，屏幕上会显示 SCAN 的应用说明如下：

SCAN [object1] [object2...] [option1] [option2...]
Options:

/?	Display this help screen.
/ADL	Scan all local drives.
/ADN	Scan all network drives.
/AF 〈filename〉	Store validation codes for all files into 〈filename〉.
/ALERT 〈server〉	Alert 〈server〉 on infected files.
/ALL	Scan all files.
/APPEND	Append to report file rather than overwriting.
/AV	Add validation code to executable files.
/BOOT	Scan boot sector and master boot record only.
/CF 〈filename〉	Check validation codes stored in 〈filename〉 by /AF.
/CLEAN	Clean viruses from infected files and system areas.
/CV	Check validation codes added to files by /AV.
/DEL	Delete infected files.
/EXCLUDE 〈filename〉	Do not add validation codes to files listed in 〈filename〉.
/FAST	Faster scanning (may miss some infections)
/FREQUENCY 〈n〉	Do not scan [n] hours after the previous scan
/HELP	Display this help screen.

/LISTEN 〈server〉	Load SCAN and wait for command from 〈server〉.
/LOAD 〈filename〉	Load options from file.
/LOG	Save date and time of the current scan to the log file.
/MANY	Scan Many Floppy Diskettes.
/MEMEXCL hhhh[- hhhh]	Exclude memory area from scanning
/MOVE 〈directory〉	Move infected files into 〈directory〉, preserving path.
/NOBREAK	Disable Ctrl-C / Ctrl-Brk during scanning
/NOCOMP	Do not scan compressed files internally
/NOEMS	Do not use EMS memory for data.
/NOEXPIRE	Disables data files expiration date notice
/NOMEM	Do not scan memory for viruses.
/PAUSE	Pause at end of each screen page.
/PLAD	Preserve Last Access Dates on Novell NetWare drives.
/REPORT 〈filename〉	Report names of viruses found into 〈filename〉.
/RF 〈filename〉	Remove validation codes from 〈filename〉 created by /AF.
/RPTALL	Include all scanned files in the /REPORT file
/RPTCOR	Include corrupted files in /REPORT file.
/RPTERR	Include errors in /REPORT file.
/RPTMOD	Include modified files in /REPORT file.
/RV	Remove validation codes added to files by /AV.

/SHOWLOG	Display date and time information from the log file.
/SUB	Scan subdirectories
/VIRLIST	Display virus list.

CLEAN.EXE 是 SCAN.EXE 软件包中的杀毒软件，其功能与其它杀毒软件类似，不再做详细介绍。但应该注意有很多 SACN 查出的病毒 CLEAN 消除不了。

尽管 SCAN 是比较优秀的查病毒软件，但在长期使用中发现与其它软件比较 SCAN 的误报率相对较高。很多用户都知道 SCAN 误报编辑软件 WS.COM 和 213 汉字的 PRT.COM 含有 FamR 病毒，结果是虚惊一场。后来又发现了 SCAN 对 Little Red(即 DABI 病毒)和 1554 等病毒判断不准。

6.4　华能 AVC-II 型反病毒卡

90 年代以来我国反病毒企业相继研制了多种防病毒卡，影响较大的有华星、瑞星、华能等牌号。这些防病毒卡的功能大同小异，以华能 2.0 卡为例说明其使用方法。

华能 AVC-II 型反病毒卡是北京华能地学高技术联合公司研制生产的反病毒产品，可以对计算机内存动态病毒进行自动检测、自动过滤并能自动清除引导型病毒。经用一些病毒实测，华能卡对微机的保护作用比较完善，兼容性好，并可用于 NOVELL 网，是一种整体功能较好的产品。华能 2.0 卡可以自动清除引导型病毒，但不能杀除文件型病毒，而且是根据行为共性检测病毒，所以仍应归为防病毒卡类。

一、安装华能反病毒卡

华能卡和其他各种反病毒硬卡需插到微机主板扩展槽中使用，安装硬卡一定要在微机断电情况下打开主机箱，保持反病毒卡元件方向

与其它硬卡元件方向一致，插入主机板上任一 62 线扩展插槽中，检查可靠到位后即可开启主机电源使用。

反病毒卡上的存储器要使用一段地址，长度为 8 到 16KB。微机都留有扩展地址供用户使用，在 1 兆地址的高端，从 C800 段起长度约 160KB，反病毒卡使用其中十分之一地址。华能卡上有一组短路开关用于选择卡的工作地址，出厂时调整到 CC00 段。如果防病毒卡与其他扩展卡(如汉卡)公用同一地址造成冲突，可调整反病毒卡上的地址开关解决。短路开关见图 6-9，在选择地址的时候两个短路块同时移动，自左向右共 4 个位置，分别对应 4 起始地址。有些用户对安装硬卡和选择地址视若危途是不必要的，前面说过扩展槽和扩展地址本来就是留给用户扩展功能卡用的，只要正常断电操作，一般用户完全可以安装成功，并且是一次性的。

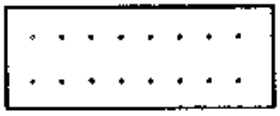


图 6-9　华能反病毒卡的地址开关

安装成功后打开微机电源，屏幕上显示如下信息：

Anti-virus card is installed! Version 2.0

Press [Esc] to close the card

下面一行是闪烁的，提醒用户可以击 Esc 键关闭华能卡，关卡后防病毒卡在本次开机过程中将不起作用，可运行一些特殊加密软件。

二、防治病毒

在微机启动过程中，启动盘(软盘或硬盘)如存在引导型病毒，华能卡自动报警：

A virus has found in Boot of the Disk A (or C)

硬盘主引导区(分区表)病毒报警信息是：

A virus has found in MBP of the hard disk

华能卡能够杀除大部分引导型病毒，杀毒后由原盘启动微机。

当由于运行带毒文件而使文件型病毒进入微机内存时，华能卡检测到内存病毒活动，发出警告并“过滤”内存病毒，屏幕信息是：

A virus has been found in XXXX

OK! The virus has been filtered.

请注意“过滤”的是微机内存中的病毒，磁盘病毒并没有消除。下次开机运行同一软件的时候磁盘病毒仍会进入内存，防病毒卡再次报警，这正是防病毒卡的特征。

三、保护硬盘主引导区和可执行文件

磁盘引导区和可执行文件是计算机病毒的主要传染目标，防病毒卡一般都具有保护引导区和执行文件的功能。当微机硬盘主引导区(分区表)将被修改时，华能卡会提示报警：

The MBP will be rewritten!

Are you sure (Y/N)?

这是一个问答式的界面，华能卡监视到 MBP 表将被修改，但不能确定修改的合法性，所以要由用户通过键盘输入允许或者不允许的命令。只有在特殊需要的时候，才能在专业技术人员操作下“合法”地修改硬盘 MBP 表。一般用户在上机过程中完全没有必要也不应该修改 MBP 表，所以遇到这种报告时应该选禁止键 N，并且请专业人员协助找出原因，极有可能是病毒所为。

当可执行文件将被重写时，华能卡的报警信息是：

The XXXX will be rewritten!

Are you sure (Y/N)?

除修改的目标不同外，这条信息的含义同上，但判断文件修改的合法性不是容易的事。病毒传染文件是一种非法修改，但不是病毒修改文件的例子也是有的。比如有些商品软件包在从软盘向硬盘安装的过程中并不是直接把所有软盘文件直接拷贝到硬盘，而要对某些可执行文件做必要的合法修改。但用户往往难于区分所谓合法或非法，因此建议当防病毒卡报告文件修改时，先选 N 予以禁止，如果微机能够顺利往

下运行，不出现异常情况，那么先前要发生的修改文件多半是病毒现象，应请技术人员深入分析；反之如果选 N 后微机运行异常，比如死机或者某些本应有的功能实现不了，那么先前发生的可能是一种合法的修改，下次开机运行同一软件防病毒卡再报警时可选 Y 试一下。

华能卡没有保护硬盘 DOS 引导区的报警信息，这可能是华能卡的一个疏忽，因为尽管为数不多，但总还是有些病毒是以 DOS 引导区为寄生地的。

6.5 求真可升级消病毒卡

92 年以前反病毒硬件技术基本上是以单纯的防病毒卡为主。93 年我国计算机工作者发明了一种硬卡在线升级技术，经国家专利机关检索在国际上尚无先例，是一项具有国际领先水平的中国发明专利。以这项先进技术为基础，电力工业部信息中心求真实验室设计开发了求真可升级消病毒卡。

求真卡的安装与华能卡类似，不同处有两点。一是求真卡的地址开关有 4 位，可搭配成从 C800 段到 EC00 段 10 种地址组合。二是由于求真卡具有杀毒、防毒双重功能，所以开机时如果选择关闭防毒功能，求真卡的杀毒功能仍将工作。

求真卡是以反病毒为主的多功能集成化卡，有从三合一卡到六合一卡的多种配置，高配置求真卡相当于把以下六种硬卡集成到一块卡上。

一、杀病毒卡

求真卡载有大型病毒特征数据库和杀病毒程序，可以有效地消杀磁盘上的引导型、文件型和混合型等病毒。杀毒时明确报告病毒名称，报警和杀毒连续进行，微机不停顿，速度很快。在开机上电阶段，求真卡发现和杀除引导型病毒的报警信息是：

!!! QZW WARNING !!!　　求真报告

Azusa virus is found in A:	A 盘发现 Azusa 病毒
Killing please wait	正在杀除 A 盘病毒
Press any key to Reboot	病毒已消除，按任意键重启微机

Azusa 是一种引导型病毒的名称，又名 2708 和香港。求真卡具有较强的广谱杀毒能力，即除已知病毒外，还能发现和杀除一些新的未知名引导型病毒。

对于文件型病毒求真卡有两种杀毒方式，主要方式是在线实时杀毒，这是发挥硬卡特长，不需要用户干予的自动杀毒方式。例如用户把新得到的一套游戏软件安装到 D 盘 GAME 子目录中，主文件名是 PLAY.EXE。当用户输入主文件名 PLAY 并回车后，求真卡即自动检测磁盘 PLAY.EXE 文件中有无病毒，若发现病毒，求真卡将报告和杀除磁盘病毒：

!!! QZW WARNING !!!	求真报告
NATAS virus is found in D: \ GAME \ PLAY.EXE	在 D 盘 GAME 子目录 PLAY.EXE 文件中发现 NATAS 病毒
Killing please wait	正在杀除 D 盘 PLAY.EXE 文件中的病毒

NATAS 是 95 年最新发现的复杂变形病毒，杀除磁盘病毒后，报警信息将从屏幕上消失，恢复屏幕原来的字符信息，自动运行杀毒后的无毒 PLAY.EXE 文件，整个过程连续进行，无需人工干预。

有些病毒重复感染文件，例如黑色星期五病毒无限制地感染 EXE 文件，因而又称疯狂拷贝病毒，变种 FLIP 也有同样性质。病毒之间还会交叉感染，即一个文件被多种不同的病毒感染。对于重复和交叉感染病毒，求真卡会一层层地把它们消除，最终得到一个无毒文件。杀除交叉感染病毒的示例如下，两次报警和杀毒是连续的。

```
!!! QZW WARNING !!!
1575 virus is found in C:JIAO.COM
Killing please wait
```

!!! QZW WARNING !!!

JERUSALEM virus is found in C:JIAO.COM

Killing please wait

除在线自动杀毒方式外,求真卡还提供特殊命令 DIR QZKL 用于检测和杀除磁盘当前目录中所有文件型病毒。利用这个命令编成批处理文件可以方便地杀除整个硬盘或网络服务器上的病毒。杀除网络服务器病毒示例如下:

!!! QZW WARNING !!!

DOCTOR virus is found in E: \ DEBUG.COM_(REMOTE)

[Y] = Yes [N] = Not?

文件名后的(REMOTE)表示是远程服务器,选项主要根据本地机的权限确定。

二、防病毒卡

与华能卡一样,当遇到未知新病毒时,求真卡具有报警,防止病毒扩散破坏的功能,也就是起普通防病毒卡的作用。

发现新病毒的报警信息:

!!! QZW WARNING !!!	求真报告
A virus is found in XXXX	发现由 XXXX 文件带入内存的未知名新病毒
The virus is removed	内存病毒被移出
Press any key to continue	击任意键继续

求真卡和优异卡都是可升级卡,防病毒只是遇到未知新病毒时的一种临时对抗方式,可以通过卡的自升级性追加消杀新病毒的能力。

保护硬盘主引导区(分区表)和 DOS 引导区的报警信息:

!!! QZW WARNING !!!	求真报告
C:BOOT sector will be modified	硬盘引导区将被修改
[Y] = Yes [N] = Not ?	选项

保护磁盘重要文件(COM、EXE、OVL、BIN、SYS 等)的报警信息:

!!! QZW WARNING !!!	求真报告
XXXX will be modifed	XXXX 文件将被修改
[Y] = Yes [N] = Not ?	选项
!!! QZW WARNING !!!	求真报告
XXXX will be deleted	XXXX 文件将被删除
[Y] = Yes [N] = Not ?	选项

微机硬盘主引导区、DOS 引导扇区是开机过程中最先读取的两个磁盘扇区，微机的设置状态(各种设备类型、内存容量、密码等等)保存在 CMOS-RAM 存储器中，显然硬盘引导区和 CMOS-RAM 对微机至关重要。为了保护硬盘引导区和 CMOS-RAM 设置，求真卡可以为它们建立备份，方法是用一片不带写保护的系统软盘启动微机，在开机后显示求真版本说明的十个光点标尺过程中击一下 Tab 键，屏幕上将显示 QZW.COM is constructed，开机后自动在启动盘根目录下生成一个名为 QZW.COM 的文件，长度为 1280 字节，其中备份了硬盘引导区和 CMOS-RAM 中的微机设置数据。以后在需要的时候运行一下 QZW.COM 文件就能恢复微机硬盘引导扇区和 CMOS-RAM 设置。

三、自升级(编程)卡

各种反病毒卡的功能是以指令代码和数据形式存放在卡上的固态存储器中，所谓升级就是用功能更强的指令代码和新的数据去修改或补充卡上的固态存储器。以往防病毒卡的升级是由销售商使用另外一种专用设备——编程卡完成的，也就是说防病毒卡只管防毒，编程卡只管升级，两者是分离的。编程卡的价格在千元以上，防病毒卡用户显然不可能为了自己升级而另配一块编程卡。求真卡把杀毒卡、防毒卡和编程卡的功能集成到同一块硬卡上，从而使其本身成为可升级的自编程卡，用户自己进行简单的操作就能为求真卡升级升版，扩展新的功能。

升级的具体方式是由研制单位定期在<中国计算机报>、<软件报>、<电脑爱好者>等媒体上发布"求真反病毒升级公告"，内容包括

对新病毒分析和升级数据清单。以下是曾经公开发表的 0026 号升级数据清单：

```
100 REM KILL 109X VIRUS
110 DATA 0A,50,5A,57,20,43,41,52,44,00,00,00
120 DATA 02,B8,01,28,00,B9,DA,00,BE,11,03,6A,54
130 DATA 07,E8,BE,00,31,30,39,58,00,62,74,62,74,0C,07,26
140 DATA 00,00,00,01,27,29,2B,2D,0C,07,26,00,00,0B,27,01
990 DATA END,1483,1561,002
```

这段升级数据用于杀除 1091 和 1099 恶性病毒，即在此次升级前求真卡防治了进入内存的 109X 病毒，禁止其传染和激发，而升级后将杀除磁盘文件中的 109X 病毒。可以看出升级数据是一段简短的 BASIC 程序，用户按清单输入与公用的升级主程序连接后运行一次就完成求真卡的升级。由于求真升级公告公开发表，所以任何用户只要订阅报纸就能免费获得升级数据。求真卡的升级数据还可通过软盘通讯传递，软盘上是可执行 COM 文件，使用更为方便。据报道从 94 年 7 月到 95 年 9 月求真卡共发布 30 多次升级公告，防治和追杀了幽灵、Casper、NATAS 等一批国内新发现的病毒。除追杀新病毒外，集成化卡的升级还包括卡的综合性能改善等。

求真卡设有升级自锁开关，升级数据内含多种校验码，以保证升级在用户本人控制下可靠进行。

四、固化 DOS 卡(硬盘仿真卡)

微机开机后有一个 DOS 引导过程，能够引导开机的磁盘称为引导盘或者系统盘，带/S 参数格式化的磁盘，包括硬盘 C 和软盘就是 DOS 引导磁盘。引导盘上有三个系统文件，一个是 COMMNAD.COM，另外两个是隐含的。这三个文件以及引导扇区非常重要，也最容易受到损伤。明显的原因有两点，一是成为病毒传染攻击的主要目标。现存两大类病毒中，引导型病毒就是以传染引导区而命名的；另一类文件型病毒则大多把 COMMAND.COM 文件作为首选传染对象；二是由于每次开

机都读取引导扇区和系统文件，容易造成物理损伤，磁盘"0 磁道坏"的几率远大于其它磁道，其原因正在于此。

所谓固化 DOS 是指把开机引导所必须的三个系统文件固化到硬卡上，使得开机引导过程既不用硬盘 C，更不用软盘，而由硬卡引导微机。用固化 DOS 引导微机，具有速度快、可靠性高、保证微机无毒启动、延长驱动器寿命、驱动器损坏时仍能开机等优点。

求真卡可以固化 DOS，在固化 DOS 引导过程中，DOS 系统文件从求真卡上读出，CONFIG.SYS 和 AUTOEXEC.BAT 则从硬盘或软盘上读出，以适应用户配置的要求和变化。

五、国家标准汉字库卡

求真卡可以固化国家标准 16 点阵二级字库汉字及符号 8 千余个，挂接 2.13、UCDOS 等常用汉字操作系统。字库由求真卡提供，读取速度快于磁盘，不占微机基本内存、扩展内存、软硬盘等任何资源，为用户节省 256KB 基本内存，也不会与其它使用扩展内存的软件冲突，可运行各种大型汉化软件。

六、光盘伴侣卡

求真光盘伴侣原是求真实验室于 1995 年 8 月推出的磁盘软件，作用是提高光盘使用效率，为用户节省硬盘空间。发行后用户反映很好，所以移植到求真卡上，功能特性较纯软件有所提高。

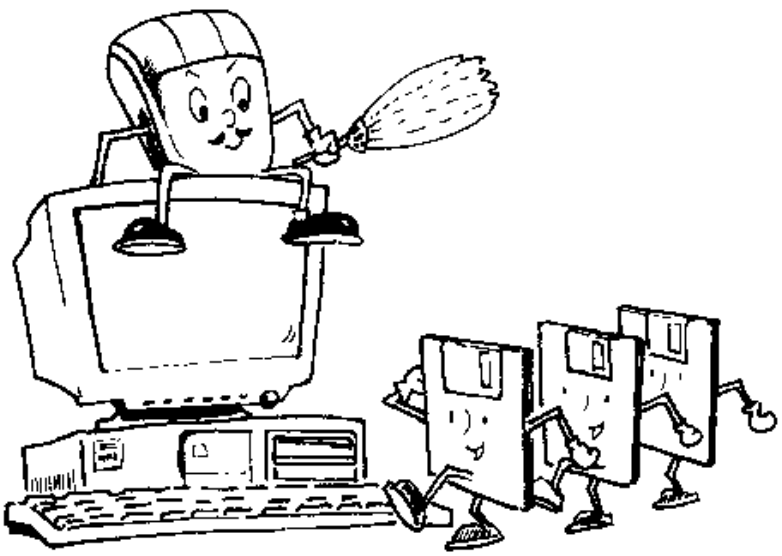
由于光盘 CD-ROM 是可读而不可写的，所以大量的磁盘软件制作到光盘上后不能正常运行，用户不得不把软件从光盘拷到硬盘去使用，浪费了大量硬盘空间。光盘伴侣是为解决 CD-ROM 不可写问题而设计的系统，支持用户直接使用光盘上的软件。举例来说，几乎所有的游戏软件都需要记录游戏进度或成绩，CD-ROM 不能存储进度成绩，所以光盘上的很多游戏软件是不好用的，而要拷贝到硬盘上。在光盘伴侣支持下则可直接使用光盘上的游戏软件，在存储进度的时候会自动存到用户指定的磁盘上（软硬盘及硬盘的子目录均可）。用户指定的磁盘与

光盘相辅相成，光盘管读出，磁盘管写入，两者相依为伴，故称光盘伴侣。

求真卡的第五、六项功能与计算机病毒没有直接关系，所以只做了最简单的介绍。但这两项功能的实现对反病毒产品的发展却有影响。用户配置反病毒产品是一种必要的安全保险措施，由于用户安全意识的增强和反病毒技术的发展，即使遇到病毒也会很快清除，所以在大部分时间内微机是无毒运行的，这就产生了反病毒卡的多功能利用问题。以防病毒卡为例，防病毒卡占用微机的一个插槽，只有防病毒一项功能，微机有毒时固然起防毒作用，微机无毒时防病毒卡干什么呢？求真卡集成多项功能，达到了微机有毒时杀毒防毒，无毒时还能为用户提供其他有用功能，一卡多能代表了反病毒产品的发展方向。

第七章

病毒与反病毒热点问答



问:为什么非系统软盘会感染引导型病毒?

答:微机所用的软盘分为系统盘和非系统盘,系统盘是用 FORMAT /S 命令格式化的,盘上有 COMMAND.COM 和另外两个隐含的 DOS 系统文件,可以引导微机开机进入 DOS 操作系统。非系统盘用不带 S 参数的 FORMAT 命令格式化,不能引导微机开机。不管是否是系统盘,软盘的第一个扇区都是 DOS 引导区,因而都可能感染引导型病毒。在微机内存带毒情况下读写软盘,病毒并不管是不是系统盘一律进行传染。当误用带毒的非系统软盘启动微机时,染毒的引导扇区首先被读出,病毒进入内存后立即传染硬盘。所以尽管非系统盘尽管不能引导开机,但硬盘已经染毒,以后每次开机硬盘引导区病毒都要进驻内存。

问:什么是 DIR-II 病毒?

答:DIR-II 是一个非常出名的病毒,很多关于病毒的书籍文章中都要点它的名,对于 DIR-II 可以列出一连串与众不同的特点:

1.从病毒机理上说 DIR-II 是第一个不修改任何中断向量获得系统控制权的病毒。由于人们事先没能预计到这种新原理病毒的出现,所以 DIR-II 病毒冲破了当时几乎所有防病毒卡的防线。

2.在寄生方式上 DIR-II 病毒不同于其它文件型病毒,其它病毒都是作为外壳寄生在每一个传染文件上,而 DIR-II 病毒寄生在磁盘的最高簇,每个磁盘只有一个病毒体,所有染毒文件公用这个病毒体。

3.DIR-II 病毒的有效长度只有 400 多字节,属于最短的病毒之列。

4.DIR-II 的传染速度快,可一次传染所列目录下的所有可执行文件。由于硬盘上染毒文件多,如果杀毒不彻底其复发率很高。

5.DIR-II 病毒传染文件的时候对原文件不做任何修改,而是改动文件目录表中的首簇号,使其指向磁盘最高簇的病毒体。

6.在微机内存无毒情况下如果拷贝被 DIR-II 病毒感染的文件,所拷贝的只是病毒,不管原文件多长,拷贝的文件只有 1024 或 2048 字节长,即病毒本身,真正的原文件全部丢失。

问：通过列目录方式传染的病毒之间是否都是变种关系？

答：早期的文件型病毒是通过加载执行文件传染的，后来出现了通过列目录过程传染的病毒。较早发现的几个列目录传染病毒就用 DIR 命名，比如 DIR 病毒、DIR-II 病毒。以后列目录传染病毒越来越多，再用 DIR 加一个数字表示它们就会造成混乱，也不能说列目录传染的病毒都是变种关系。例如 1575 和 DIR-II 都是列目录传染的病毒，但它们的原理及代码完全不同。

问：什么是变形病毒？

答：变形病毒在国外又称多态病毒，是计算机病毒向更深层次隐蔽自己发展而产生的一种"高级"怪胎。

前面在介绍计算机病毒的解密模块时曾经说过，很多病毒以加密形式存储在磁盘上，并且加密病毒必然有一个解密模块。加密病毒由密码和明码两部分组成，明码就是解密模块。密码部分千变万化是容易理解的，否则也就称不上为加密了。但有些病毒作者不满足于密码部分的变异，想方设法使病毒可执行的明码部分也自动产生变化。为了深刻理解可执行程序自动变化的含义，我们举一个例子进行说明。

假定教师要求学生用 BASIC 语言编一个画圆的程序，全班学生都完成了作业，但其中有一位学生编制的程序十分奇特，新奇在什么地方呢？比方说他所交的作业打印出来有 50 条语句，程序运行的结果十分正确，确实画了一个圆。奇在程序运行一次后再打印的程序清单与上一次清单不一样。所用的变量、语句的顺序、功能、甚至语句条数都有变化。虽然清单变化了，但程序的功能没有变，再运行一次照样画出圆来，而且清单又变化一次……。以此类推，这个学生编的程序在运行的时候既完成了画圆的工作，又能自动变化出成千上万个不同的清单来。

变形病毒明码解密块的变化特性与上面举的画圆例子完全相同。变形病毒每传染一次其密码和明码部分都自动变化，造成每一个磁盘病毒体看上去与另一个病毒体不同，增加了检测分析的难度。变形病

毒的明码部分程序形式虽然变化但功能不变，都是对密码部分进行解密。下面是幽灵变形病毒传染同一个文件变体的第一段程序：

第一次传染

```
00E8 36          SS:
00E9 F9          STC
00EA F5          CMC
00EB FB          STI
00EC 50          PUSH AX
00ED E9C100      JMP 01B1
```

第二次传染

```
0566 F8          CLC
0567 F8          CLC
0568 50          PUSH AX
0569 FD          STD
056A E9EF03      JMP 095C
```

变形病毒的编制难度很大，就其创意来说也不是人们一般能想象的，可以肯定变形病毒的编制者具有很高的编程水平。

问：幽灵病毒究竟有多少种？为什么95年一下子冒出好几个幽灵病毒？

答：1994年3季度中关村地区的一些计算机公司和高等学校发现有一种新病毒流行。新病毒行为诡秘，一些著名的反病毒软件也检测不到它，经中科院有关专家分析，这种新病毒属于国际上盛传已久的变形病毒，也称多态病毒。新病毒长度为3544字节，是既传染可执行文件又传染硬盘主引导区的双料病毒。根据新病毒诡秘多变的特性，有关专家将其命名为“幽灵”。

根据有案可查的资料，“幽灵病毒”第一次出现在计算机专业报刊上是1995年1月14日，是日出版的《软件报》发表了题为“中国对幽灵说不”的技术专文。文章在披露幽灵病毒已经入境的同时宣布幽灵在

我国的传播途径已被堵死，我国专家在极短的时间内就解决了幽灵病毒的检测和消除问题。

因为幽灵一词比较引人注目，后来出现的其它变形病毒有时也被称为"幽灵"，如 Casper 幽灵、幽灵 2、NATAS 幽灵王等等，其实这些病毒与中科院专家命名的幽灵病毒并没有什么关系。

问：什么是网络病毒？怎样防治网络病毒？

答：对于网络病毒有两种解释。一是目前已发现很多在单机上运行的病毒被拷贝到网络服务器上，各工作站在使用服务器上的带毒文件时，工作站内存就会带毒，传染工作站硬盘上的其它文件。由于网络是高度共享的，病毒会很快在各个有盘工作站上扩散。二是针对网络系统编制的病毒，其传播的速度和对网络的破坏性更大，但国内尚未报道发现此类病毒。

网络系统应该建立完善的信息安全管理制度，根据需要严格规定各工作站的读写权限，只有网络管理人员才有权向服务器上安装软件。

常用的杀毒工具，如 KILL、CPAV 杀毒软件、求真消病毒卡都能检测和杀除网络服务器上的病毒。应该注意的是一旦发现病毒就应该对服务器和各工作站统一查毒杀毒，否则病毒可能会很快再次感染网络。最好指定一台工作站对服务器进行经常性检查。另外还有一些网络专用的防毒、杀毒产品，可以实时检查进出服务器的数据。

问：在报刊上曾看到关于 CMOS 病毒的提法，究竟有没有 CMOS 病毒？

答：CMOS 是微机中的一种特殊存储器，记录了微机的硬件设置参数及系统日期时间、开机密码等重要数据。由于 CMOS 设置十分重要，所以可能成为计算机病毒破坏攻击的目标。但 CMOS 中不会有病毒寄生，因为：

1. CMOS 是通过 I/O 读写与 CPU 交换数据的，CPU 的物理机能决定了只能读写 CMOS 的数据，不能把 CMOS 中的数据当作指令代码来

执行。

2. 如果把一段病毒程序写入 CMOS，则必然破坏微机的硬件设置以至于微机根本就不能运行，存储在 CMOS 中的“病毒程序”将毫无作用。

3. CMOS 的有效存储容量只有 128 个字节，不足以容纳病毒。

问：有没有破坏硬件的计算机病毒？

答：国内还没有发现。国外已经发现能够破坏计算机硬件的病毒。当然硬件受损必定有物理原因，所以病毒不可能随心所欲地选择破坏目标，至少纯数字电路是安全的；但从机理上分析，微机中有些硬件部位可能成为病毒的攻击目标。

问：有没有可以到处传播而又杀除不了的病毒？

答：没有。如果有这种病毒，那么总有一天它会传遍全世界所有的计算机系统，而全世界计算机界和用户却对它无能为力，计算机科学岂不要“死亡”了？

问：光盘会带计算机病毒吗？

答：光盘是一种新型存储介质，具有容量大，可靠性好，性价比高等优点。光盘有可擦写光盘和只读光盘两种，可擦写光盘价格十分昂贵，目前应用还不广泛。普通用户使用的是只读光盘 CD-ROM，CD-ROM 上的软件数据是光盘制造厂使用专用设备写到盘片上的，用户使用的时候只能读出光盘上的软件数据，不能向光盘存储新的数据和文件，所以 CD-ROM 在使用过程中不会被病毒传染。但有些光盘确实带有病毒又是怎么回事呢？这是光盘制造厂在制作光盘时把关不严，把带毒的软件做到光盘上造成的。光盘生产厂都是具有一定规模的企业，而制造出带病毒的产品，说明了计算机病毒真是无孔不入。由于光盘不可改写，病毒会传播到各地，后果是很严重的。

国内第一例光盘病毒发现于 95 年 3 月，当时一台微机在未使用外

来磁盘软件的情况下突遭病毒袭击，丢失了硬盘。经特殊处理修复硬盘后发现很多硬盘文件都含有 1099 病毒。根据用户提供的线索，找到一片名为〈软体荟萃〉的光盘 TOOLS 子目录中一些文件含有同一种病毒。95 年下半年又发现〈XX 软件大补贴〉带有恶性病毒，所以在使用光盘时不能掉以轻心。

问：怎样检查和处理光盘上的病毒？

答：从原理上说各种具有查毒功能的软硬件产品都可以用来检查光盘上是否存在计算机病毒。针对 CD-ROM 的特点，查毒可注意以下几点：

1. 光盘容量很大，有些光盘甚至有上万个文件，全部扫描一次要 20 分钟到半小时，用户可能不愿意花费这样长的时间，可重点检查 COM 和 EXE 文件。

2. 选用具有查毒功能的求真、优异卡可不必事先检查整片光盘，因为这些卡是实时工作的，可以随时查出光盘上的静态病毒。上面提到的国内第一例光盘 1099 病毒就是求真卡实时检测到的。

3. 由于 CD-ROM 是不可改写的，所以反病毒工具可以检测发现光盘上的病毒，但无法杀除病毒。解决的方法是把带毒的光盘软件拷贝到硬盘上，再用杀毒工具杀毒。当然以后应使用硬盘上杀毒后的软件，而不要用光盘上的带毒软件。

问：为什么有时用杀毒软件杀毒后微机上很快又出现同一种病毒？

答：原因可能是：

1. 只杀除了硬盘病毒，未处理软盘，当使用带毒软盘时病毒再次传染硬盘。

2. 只处理了硬盘的部分子目录，没有对整个硬盘杀毒，运行未杀毒子目录中的带毒软件时病毒再次扩散到硬盘其它部位。

3. 杀毒软件本身不够完善。

问:为什么硬盘格式化甚至重新分区后很快又发现病毒?

答:硬盘有两个引导区,主引导区(又称分区表)和 DOS 引导区。就引导型病毒而言,大多数病毒都侵入硬盘的主引导区,DOS 的 FORMAT 命令与硬盘主引导区无关,所以如果贸然用 FORMAT 去"杀除"侵入主引导区的病毒,除了白白损失硬盘 DOS 分区的数据文件外,对主引导区中的病毒并无任何触动。

用 FDISK 分区命令对硬盘重新分区确实能以损失全部硬盘数据为代价清除硬盘上的病毒。但 FDISK 分区后的硬盘空空如也,用户所做的第一件事就是把大批软盘软件安装拷贝到硬盘上。对单机用户来说(即不联网),硬盘之所以染毒,肯定是一部分软盘带毒所致,如果软盘病毒不清除,照样会被拷到硬盘上。

问:为什么有些染毒文件经杀毒软件杀毒后会比真正的原文件长出几个字节?长出的部分会不会留下隐患?

答:有很多文件型病毒不是紧接在被传染文件后面,而是对被传染文件的长度按微机使用的 16 进制数取整后传染。举例来说假定病毒要传染一个长度仅 12 字节的文件。在 16 进制数中 12 不是整数,病毒按 16 取整后接在长度 16 的地方。病毒与原文件末尾之间留有 4 个字节的无用数据,不论是病毒还是原文件都不会用到这 4 字节数据。杀毒软件在杀毒的时候能够准确地找到病毒的开头,但一般不知道原文件究竟在何处结尾,所以就从病毒开头的地方截断病毒,对本例来说就是从第 16 字节起清除病毒,这样杀毒后的文件长度是 16 字节,而不是 12 字节。显然长出的 4 个字节既不会影响原文件的运行,也不会留下隐患。所以通常杀毒后的文件比原文件长 1 到 16 个字节是正常现象。

问:为什么有些文件带毒时不能运行,而经杀毒软件杀毒后又可以运行?

答:这主要是病毒有错误或者病毒的兼容性差造成的。有些病毒只能在低版本 DOS 下运行,一个染毒文件从使用低版 DOS 的微机上拷

贝到使用高版 DOS 的微机上--运行就会死机。而杀毒后病毒的不兼容性被排除，则只要软件本身适应于高版 DOS 就能顺利运行。病毒有错误的情况与兼容性问题类似(兼容性差本身也可以说是错误)，有可能通过杀毒解决。所以染毒文件不能运行并不一定是文件被破坏，不妨杀毒试一下，或许能有意外收获。

问：为什么杀毒软件容易被病毒感染？

答：根据统计，在各种软件中杀毒和查毒软件感染病毒的机率较高。这一现象有点奇怪，杀毒软件本来是病毒的克星，为什么反被病毒感染呢？实际上这主要是对杀毒软件使用不当造成的。有些用户在微机有染毒迹象时，习惯于立即用查杀毒软件去检查，如果微机内存中确实有病毒活动，则不管查杀毒软件能否识别病毒，杀毒软件都会被病毒感染(在不加写保护状态下)。特别是当杀毒软件不能识别新病毒时不会有任何报告，而杀毒软件本身已经染毒。

用带毒的杀毒软件去查毒杀毒，由于扫描一个个子目录甚至全盘，病毒会在扫描过程中迅速传染整个硬盘，危害很大，所以一定要注意正确使用查杀毒软件：

1.在需要使用查杀毒软件的时候，应该用无毒系统软盘启动微机，以保证微机内存“干净”。

2.查杀毒软盘一定要写保护，尽量不在硬盘上启动查杀毒软件。

3.使用正版软件并及时要求供应商予以升级。

问：防病毒卡能够保证计算机“带毒安全运行”吗？

答：防病毒卡具有一定防护作用，但把“带毒安全运行”作为防病毒卡的功能指标是有害的。因为首先防病毒卡并不能防治所有新病毒，当防病毒卡发现不了新病毒时，显然不能保证微机安全运行。其次即使防病毒卡能够发现病毒，所能采取的保护措施也是有限的，而不会是无限的。比如 94 年发现的 1855 病毒看起来很平常，有的名牌防病毒卡虽然可以检测到它，却不能阻止传染重要的 COMMAND.COM 文件。

再者某些病毒错误造成的死机等不正常现象用防病毒卡是解决不了的。所以当防病毒卡报告发现病毒时应尽快用杀毒软件查毒杀毒或者与反病毒专业部门联系，而不要强行“带毒运行”。

问：什么是“病毒前报”？

答：“病毒后报”和“病毒前报”是关于防病毒卡报告发现病毒时机差别的说法。让我们通过具体例子来进行说明。假定字处理软件 WS.COM 感染了病毒，当微机运行 WS 时病毒将立即进入内存。早期的防病毒卡在 WS 工作过程中并不报告发现病毒，而是在用户停止使用 WS 的时候报告，也就是在染毒文件运行结束后报警，这种报警方式叫作“病毒后报”。病毒后报方式判断病毒的准确性相对好一些，但从用户开始使用 WS 到退出 WS 可能有相当长一段时间，防病毒卡在这段时间内又未报告发现病毒，所以如果病毒在用户用 WS 编写文章的过程中激发将造成严重破坏。后来防病毒技术有所发展，当病毒随染毒文件进入内存时，能较快地发现报警，而不需要等到染毒文件中止运行再报告，这种报警方式叫作“病毒前报”。所以“病毒后报”和“病毒前报”是以染毒文件是否结束运行为标准来划分的。

如果以病毒是否进入内存为基准进行观察，防病毒卡总是在病毒进入内存后才能报警。只有实时在线监测的杀病毒卡才能在磁盘病毒侵入内存前报告发现病毒并予以杀除，使加载到内存中的是一个无毒文件。

问：防病毒卡究竟是主动防病毒还是被动防病毒？

答：在防病毒卡的产品宣传、性能介绍中经常提到防病毒卡可以“主动防治病毒”；而在一些反病毒技术专文中又会看到对这种说法的批评，认为防病毒卡对病毒的反应完全是被动的，产生上述截然相反观点的原因是观察点的不同。

对于杀病毒软件来说，总是病毒出现在前，技术人员对病毒样本分析在后，编制出相应的查杀毒程序。而防病毒卡能够防治一些新病毒，

或者说在某些新病毒出现之前防病毒卡已经具备防治它们的能力。所以推崇防病毒卡的观点认为杀毒软件是被动的，而防病毒卡能主动防治病毒。

另一方面推崇杀毒软件的观点则认为用户及时用杀毒软件去检测杀除外来软件中的病毒，病毒就不可能进入用户微机内存，所以是主动杀毒；而防病毒只能在病毒经进入内存后才能报警，所以防病毒卡是被动报警防毒。

问：有一种说法"只要几条指令就能置防病毒卡于死地"，那么反病毒卡是不是很容易损坏？

答：确有这样的说法，但"死地"的含义模糊不清，只能揣测着分析：

1.如果"死地"隐喻硬卡物理损害，那么结论是否定的，即计算机病毒不可能造成防病毒卡和集成化卡的物理损伤，硬卡在物理上是坚固的。

2.如果"死地"是指造成微机死机（软件死机）等异常现象，从技术上是可以做到的，但与反病毒卡无关，因为即使不插反病毒卡的微机，病毒也可以"很容易"使微机死机，这恰恰暴露了病毒的存在。

3.计算机病毒使反病毒卡无效，而微机继续工作，这种情况就不太容易了。

问：变形病毒的出现是不是意味着特征码杀病毒技术陷入困境？

答：我国反病毒工作者对非常复杂的幽灵、CASPER、NATAS 等病毒在极短的时间内就予以封杀，有效地控制了这些病毒在我国的传播，保护了用户利益。如前面所说的，我国在首次报道幽灵病毒的时候就响亮地提出"中国对幽灵说不"。所以杀病毒技术非但没有"陷入困境"，反而是有力地回应了变形病毒的挑战。

问：在反病毒领域，软件是否将代替硬卡？

答：以往广泛使用的杀病毒软件和防病毒卡是机理功能不同的产

品，不是相互替代关系。只用杀毒软件，不用防毒卡微机就没有防治新病毒的能力；反之只用防毒卡，不用杀毒软件那么硬盘上的染毒软件就始终是带毒运行的。所以在杀毒软件和防病毒卡之间不好说谁代替谁。

同类功能产品，比如防病毒卡和防病毒软件比较，则可以肯定软件不如硬卡，在产品安全性、保密性、存储器使用等方面差距还比较大。

1.存储器使用。硬卡不占用任何内存 RAM，驻留式软件要占用几 K 到几十 K 用户内存。

2.保密性。软件驻留后是一段无任何保密措施的明码，很容易被人分析。硬卡系统也是 CPU 可直接执行的指令代码，但可利用硬件技术予以隐藏。

3.安全性。硬卡不会被病毒改写，物理上十分可靠；软件则可能被病毒改写，易受物理损伤。

4.优先级。硬卡可优先于一切磁盘病毒启动；软件则滞后于引导型和混合型病毒。

5.兼容性。两者基本相当。

问：究竟是杀毒软件好，还是防病毒卡好？

答：杀毒软件和防病毒卡都是反病毒工具，它们的功能机理不同，不能相互替代，但它们有共同的对抗目标，就是计算机病毒。中国有句俗话："上阵亲兄弟"，杀毒软件和防病毒卡正应该亲如兄弟，联合起来与病毒作战，而不应该片面夸大一方的优点，突现对方的不足，未上阵先自"内战"起来。如果反病毒阵线内部争战不休，那搞病毒的人岂不是坐山观虎斗，坐收渔翁之利吗。

问：什么是开放式反病毒？

答：开放式反病毒是指可以由用户参与的一种反病毒方式，开放式反病毒通常向用户提供或推荐某种编辑软件，当用户遇到新病毒时可以自行进行分析，利用编辑软件输入病毒的有关参数，就可以杀除新病

毒。但实际上大多数用户自行分析病毒有困难，所以新病毒参数仍由厂方提供。厂方提供的参数一般是加密的，但公开发表，用户可自行根据新病毒参数对自己使用的反病毒产品升级。开放式反病毒产品可以快速跟踪新出现的病毒，并且用户可以免费升级，因而具有较好的发展前景。

问：什么是动态杀毒？

答：动态杀毒又称仿真杀毒，是在动态病毒检测技术基础上杀除未知病毒的技术。其原理是先利用防病毒技术检测到内存中有病毒在活动，再分析病毒来源，运用覆盖或者"脱壳"技术消除磁盘病毒。动态杀毒的特点是不依赖于对病毒个体的分析，理论上可以杀除各种未知病毒，是一种较有吸引力的反病毒技术。动态杀毒必须首先准确判断病毒，继而准确清除病毒，两者缺一不可。动态杀引导型病毒的技术已经比较成熟，求真可升级消病毒卡和华能反病毒卡都具有杀除新引导型病毒的功能，而且在实际应用中得到检验。但动态杀文件型病毒尚存在两大障碍：

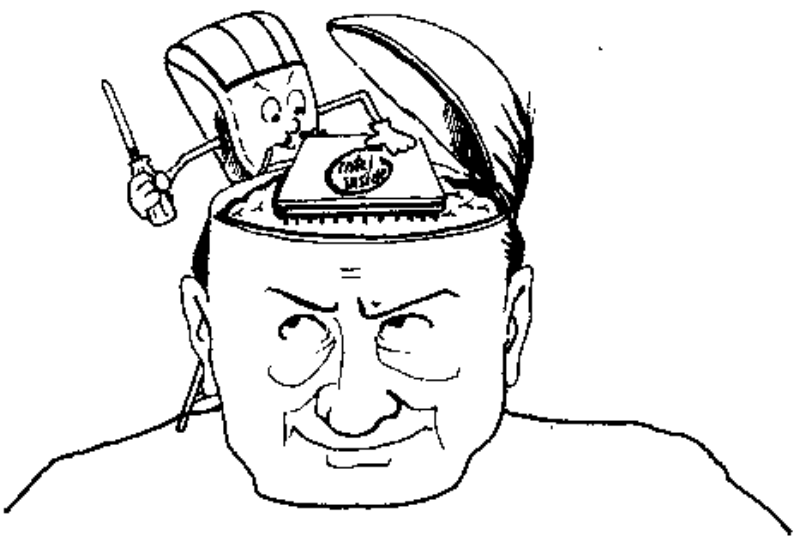
1.动态杀毒的前提是准确判断内存病毒，但各种防病毒产品对内存病毒的判断还不能保证完全准确。当内存实际无毒，而误判有毒就会把无毒文件当成有毒文件去杀毒造成无毒文件的损坏。这不符合计算机安全产品的技术要求。

2.在脱壳的时候如果不要求用户参与(即不要求用户输入参数)则难于准确脱去病毒外壳，如果要求用户输入参数则大多数用户难于操作。

尽管动态杀除文件病毒技术尚不成熟，但作为一个研究方向仍会继续发展，或许将来会出现能方便精确杀除文件型病毒的产品，那将是反病毒技术的一大突破。

第八章

流行病毒要览



尽管难以准确统计，但全世界范围内已经出现的计算机病毒可以说有上千种。随着计算机用户安全意识的增强和反病毒技术的发展，有些病毒已成历史遗迹，又有些病毒来不及大面积扩散即遭封杀。对我国用户来说真正造成威协的是已经在我国本土发现，正在流行的新病毒。本着实用求新的原则，本章介绍 1994 年以来国内发现的一部分新病毒，以便广大用户了解其特性，进行防范。这里介绍的这些病毒，我国 KILL75.03 软件和求真消病毒卡 0055 都能检测杀除它们。

一、随机格式化病毒 109X

1091 病毒 1993 年 11 月在北京地区被发现，1994 年 1 月 22 日首次公开报道。继 1091 之后，94 年上半年又发现长度为 1099 字节的变种，统称为 109X 病毒。109X 病毒激发时随机性地改写硬盘，所以又叫“随机格式化”病毒，改写后的硬盘中是一些没有任何用处的“垃圾”数据，是一个极恶性病毒。

109X 病毒驻机后截获 INT21 中断，在用户列目录时传染扩展名为 COM 和 EXE 的可执行文件，传播速度很快。病毒加在原文件的尾部，由于按 16 进数取整，所以文件长度增量为 1100 个字节上下。病毒的大部分是加密的，利用修改返回地址和屏蔽键盘中断的双重手段反跟踪。

病毒内设计数器，在病毒驻机后截获 INT8 中断进行计数，截获 INT9 中断监视击键情况。INT8 中断每秒发生 50 次，每击一键则发出一次 INT9 中断，通过两者结合，病毒监视用户击键情况，若两次击键之间的时间达一小时，则病毒激发，随机改写硬盘，破坏全部硬盘资料。激发时没有外在表现，只是硬盘灯瞬间闪亮一下，用户很难觉察，微机随即“死机”，待关机后再开机会发现硬盘已被彻底破坏。特别要指出，只要修改计数器初值，就能改变病毒激发时间。

检测内存中的动态病毒可在 DEBUG 下显示 0:53E 和 0:53F 单元中的字数据，若为 B483 则病毒已驻机，应立即关机重新无毒启动后查找染毒文件并杀毒。

检测文件中的静态病毒可用 DEBUG 调出文件反汇编，若在文件入口附近发现 DB 6A 数据，且文件长度增加约 109X 字节，可判定感染了 109X 病毒。

对于长度为 1099 的病毒，染毒 COM 文件的原前 11 个字节被保存在相对病毒头偏移 127H 处，染毒 EXE 文件的 SS、SP、IP、CS 分别保存在相对病毒头 127H、129H、12B 和 12DH 处；对于长度为 1091 的病毒，上述各偏移值均应减 8，根据这些参数和病毒长度，就可以用 DEBUG 进行手工消毒。

二、文件型 BUPT 病毒

BUPT 病毒于 1994 年 5 月在北京展览馆 94'计算机京交会上首次被发现，当时的各种杀毒软件均不能查出和杀除，94 年 7 月 23 日首次报道。计算机病毒出现在全国大型计算机展示会上，从一个侧面反映了病毒的猖獗。

文件型 BUPT 的长度为 1363 字节，在运行一个含 BUPT 病毒的文件时，利用 INT21 调用的 31 功能驻留内存，占用 2K 基本内存。驻留后的病毒截获修改 INT21 中断的 4B00 调用，即加载执行文件时进行传染。对于 COM 文件，病毒插在原文件前部，并在文件尾部加上 4 个字节标识码，文件长度增加 1367 字节；对于 EXE 文件病毒加在原文件尾部，长度增加 1363[+16]字节，文件倒数第 8 个字节起有"BUPT"字符。除 COM 和 EXE 文件外，BUPT 还感染覆盖文件。BUPT 病毒不传染 COMMAND.COM 和长度小于 600H 字节的文件；当磁盘剩余空间小于 64K 时也不传染。

病毒在 0C 单元设置了一个字计数器，每传染一次该计数器加 1，当累加至 1000H 时病毒激发，在屏幕上显示下列字符：

Hello, welcome to BUPT, 9146, Beijing!

BUPT 没有明显的破坏作用，但一些文件染毒后不能运行或运行后不能退出。值得注意的是 BUPT 中有一段字符"Only for experiment.",即仅用于实验，至于是否还有其它非实验性攻击病毒，目前还不得而知。国

内发现含"BUPT"字符的病毒已有 3 个,分别是文件型 BUPT、引导型 BUPT 和文件型 TRAVELLER 病毒。

被 BUPT 传染的文件尾部有四字节标识码 C6、CE、CB 和 C9,检查文件是否含有 BUPT 病毒可用 DEBUG 调出文件,用 D 命令观察文件尾部四个字节,如为上述标识码,则该文件已染毒。

可以通过不太复杂的操作来手工消除 COM 文件中的 BUPT 病毒,方法是用 DEBUG 调出染毒文件,把偏移 1463(此值等于 COM 文件的载入地址 100 加病毒长度 1363)起的数据移到偏移 100 处,文件长度寄存器 CX 值减去病毒长度 1363,再用 W 命令把文件写盘就消除了病毒。对于 EXE 文件,原文件的 SS、SP、IP、CS 分别保存病毒体偏移 10H、0EH、12H 和 14H 处,可作为用 DEBUG 进行手工消毒依据。

三、DABI 病毒

DABI 是长度为 1465 字节的文件型病毒,被加载后驻留在可用内存高端,拦截 INT1C 中断用于激发,INT21 中断用于传染。DABI 在进行列目录 DIR 操作时传染扩展名为 COM 和 EXE 的可执行文件。对于染软盘每次传染一个文件,若发现目录列到某文件名时有明显的停顿,就是病毒正在传染该文件。对于硬盘一次传染当前目录下的全部可执行文件,由于硬盘速度很快,传染过程难以觉察。病毒传染 COM 文件时修改文件的前 5 个字节,其中前 3 个字节改为指向病毒的转移指令,第 4、5 字节为感染标志,而原 5 个字节加密后保存在病毒偏移 524H 处。DABI 采取了隐蔽技术,在病毒驻机时看不出染毒文件的长度变化,要观察文件长度应在微机无毒情况下进行。

9 月 9 日病毒驻机后 1 小时,由病毒控制微机演奏乐曲《东方红》;12 月 26 日病毒驻机后 1 小时,由病毒控制微机演奏乐曲《浏阳河》。循环演奏造成微机不能工作。由于病毒驻机方式的缺陷造成一些重要的 EXE 文件不能运行。

DABI-A 是 DABI 的变种病毒,修改了病毒的入口代码,其它方面没有变化。

国外查毒软件 SCAN 把 DABI 命名为 Little Red(小红)病毒,但 SCAN 有误判现象,应引起用户的注意。

四、INOC 病毒

INOC 病毒源于国外,94 年 7 月国内首次报道,是长度为 1786 字节的文件型病毒。INOC 不象其它绝大多数文件病毒那样修改 INT21 中断,而截获 INT2F 中断进行传染。INT2F 是 DOS 的多路复用中断,可通过一个链式结构扩充功能。在 DOS 命令状态下,当用户敲入一组字符并按下回车键时,DOS 就调用 INT2F 中断的 AE 功能,检查用户所敲入的字符是否是扩充命令。INOC 病毒截获这一中断功能,检查缓冲区的字符串尾若是 COM 或 EXE 并且该文件还没有染毒就对该文件进行传染。传染时病毒加在原文件的尾部,原文件的前 28 个字节被移到病毒偏移 55C 处。

INOC 把染毒后文件的长度保存在病毒的 554 到 557 单元,形成一个"免疫体"。当再运行染毒文件时,病毒检查文件长度,如果大于 554 到 557 单元的记录值,就认为文件又被其它病毒感染了,于是按 554 到 557 单元的记录值恢复文件长度和 INOC 病毒的引导头。经验证,INOC 确有一定的清除其它病毒的作用,但它本身就是一个病毒,除了其非授权传染特性外,它还造成带参数加载的命令文件不能运行。

INOC 病毒的大部分是加密的,其解密手段非常特殊。通常一段解密程序不论怎样复杂,总是按地址顺序执行的。但当运行一个染有 INOC 病毒的文件时,病毒首先修改单步执行中断 INT1 地址,接着置位 80X86 CPU 标志寄存器的 D8,利用单步执行强制修改返回地址 IP,使得每次中断结束后返回同一地址。由于 INOC 十分狡猾的反跟踪手段,使得分析人员用 DEBUG 的 T 命令跟踪或用 P 命令运行到按常规估计的解密后地址都不能成功。

判断 INOC 病毒的方法是检查文件长度,如果增长 1787 到 1833 字节,并且文件的倒数第 160 字节起有文件本身的名字,则可判定感染了 INOC 病毒。病毒偏移 558 处是染毒前的原文件长度高 16 位,55A 处是

原文件长低 16 位，偏移 55C 起 28 个字节是原文件头，根据这些参数，就可以用 DEBUG 进行手工消毒。

五、RS232 病毒

RS232 病毒从 94 年上半年起在国内流行，传染性很强，传染机制复杂，并且破坏干扰微机工作。

RS232 的基本长度为 1349 字节，当在微机上使用染毒文件时，病毒占据基本内存高端，截获 INT21 中断进行传染破坏。RS232 病毒采用多种方式进行传染：(1)在运行一个染毒文件时，立即传染 A 或 C 盘上的 COMMAND.COM 文件；(2) 病毒驻机后，用 INT21 的 4B00 调用加载执行一个无毒文件时，传染该文件；(3)截获 INT21 的 11 或 12 调用搜索文件，在 DIR 列目录时进行传染。以上基本上包括了文件型病毒的全部传染方式。

RS232 病毒内设一计数器，每次传染计数器加 1 。传染时以病毒基本长度 1349 加上该计数值作为传染长度，即第 N 次传染的文件长度增量为 1349 + N 个字节。由于 N 值逐次增加，染毒文件长度增量是变化的，可以是 1349 到 65535 之间的某一值。当然加在病毒尾部的数据对文件及病毒的运行都不会有什么影响，而 RS232 之所以采用变长度传染的方式，完全是为了造成混乱和用户判断错误。通常各种文件型病毒传染时的长度都是不变的，很多病毒都用其长度命名，并以此作为判断病毒的主要依据之一。RS232 采用变长度传染的手段则使按长度判断病毒种类的经验方法失效。但在另一方面，被 RS232 感染的 COMMAND.COM 长度又不变，这里说的不是病毒长度，而是文件长度。原来各种版本 DOS 的 COMMAND.COM 文件尾部都有一连串 0，其作用尚不甚清楚，但却给了病毒以可乘之机，RS232 正是借此自己直接嵌入 COMMAND.COM 尾部，从而使染毒 COMMAND.COM 文件长度没有任何变化。这样不论内存是否染毒，都不能根据长度判断 COMMAND.COM 文件是否染毒。

RS232 激发时破坏打印机和 RS232 串行口地址，造成使用 RS232

口的 MODERM、鼠标、绘图仪、扫描仪等不能工作。

六、BACKFORM 病毒

BACKFORM 是 94 年底发现的新病毒，95 年 2 月首次见报。

BACKFORM 长度为 1855 字节，没有加密，看起来貌不惊人，似乎很容易分析防治，然而令人想不到的是看似简单的 BACKFORM 却突破了很有名的防病毒卡的防线。

BACKFORM 传染 COM 文件的情况比较特殊，如果文件起始处不是 JMP 转移指令，病毒修改前 4 字节，1 到 3 字节被改成跳转到病毒的 JMP 指令，第 4 字节置 FF 作为染毒标志；然而多数 COM 文件开始就通过 JMP 转到第二地址，在这种情况下 BACKFORM 修改第二地址起的 4 字节。此外 BACKFORM 病毒采用与 RS232 病毒相同的手段感染 COMMAND.COM 文件，使染毒文件的长度并不改变。

BACKFORM 截获 INT21 中断，但不象其它文件病毒那样监视 11、12、3D、4B 等调用，而控制 3C、5B 和 3E 调用。BACKFORM 被加载时立即传染 COMMAND.COM，而对其它文件的传染条件不太容易满足。检查 COMMAND.COM 是否染毒可观察其第二执行地址，若为一条 JMP 指令加一字节 FF 数据，则感染了病毒。COMMAND.COM 总是有备份的，可拷贝备份覆盖掉染毒文件。

七、变形病毒 DOCTOR

DOCTOR 被认为是国内发现的第一例变形病毒，用 DEBUG 观察一个 DOCTOR 病毒可以看到它的大部分是加密的，而只有一小段十几条“裸露”的合法指令用于对加密部分解密。DOCTOR 病毒在其解密段中有意使用了空操作指令 NOP，利用 NOP 指令位置变化不影响运行的特点，每次传染 NOP 的位置循环移动一条指令位置，相应地其前后其它指令也发生移动。以这种方式 DOCTOR 会自动产生 12 个变异病毒体，它们的顺序结构各不相同，给检测杀除造成很大障碍。

DOCTOR 是文件型病毒，传染扩展名为 COM 和 EXE 的命令文件，

同时还感染可执行的覆盖文件。感染 EXE 文件时，病毒接在原文件尾部，使文件长度增加 4361 字节。感染 COM 文件的情况比较特殊，4105 字节长的病毒占据文件前部，但原文件不是整体后移，而是把被病毒所占据空间的原文件部分移到文件尾部。

DOCTOR 病毒随染毒文件加载后，占据 5360 个字节基本内存，截获 INT21 和 INT8 中断。通过 4B 调用感染尚未染毒的文件，在列目录时遇到染毒文件，减去病毒长度再显示在屏幕上，看上去文件长度并未变化，以欺骗用户。病毒内设时间计数器控制激发，激发时破坏打印通讯接口，造成微机不能正常工作。病毒的表现部分是一段关于医生和病人之间的对话，DOCTOR 病毒因此而得名。

检测内存中的动态病毒可用 DEBUG 显示 INT21 和 INT8 中断的地址，若其偏移值分别为 09F0 和 0901，则 DOCTOR 病毒已经侵入微机内存。

检测文件中的静态病毒可先在系统无毒情况下用 DIR 命令列目录，检查文件长度，如果文件增长，而且增加量符合 DOCTOR 病毒的传染规律，可基本判断染毒。为进一步确认，用 DEBUG 调出文件反汇编，若在文件入口附近发现下列指令：

```
……
MOV SI,0100
……
ADD SI,18
……
MOV AX,0FF1
……
```

则可判定感染了 DOCTOR 病毒。由于 DOCTOR 是变形病毒，所以上述指令的位置并不唯一固定。

八、幽灵病毒

幽灵病毒约在 94 年下半年传入我国，是我国境内发现的第一个复

杂变形病毒。幽灵的国外名称是 one half，因为它在表现的时候显示 Disk is onehalf 字符。

幽灵兼有文件型病毒和引导型病毒的双重特性，是混合型的双料病毒。幽灵对可执行文件的传染机制与其它已知病毒完全不同。绝大多数文件病毒是作为一个单一外壳附加在被传染文件上，而幽灵传染文件时共构成 11 个病毒段，其中有 10 段插入被传染文件，各段不仅每次传染的地址不同，甚至其执行顺序也不相同。11 段病毒代码数据每次传染没有连续两个字节是相同的，其中插入文件的 10 段都是透明的可执行代码。染毒文件长度增加 3544 字节。引导型幽灵占据硬盘 8 个扇区，在每次开机引导过程中，病毒按从高柱面到低柱面的顺序都对硬盘的两个柱面进行数据处理。经过若干次(与硬盘容量有关)开机后，整个硬盘就都处在幽灵控制之下。经病毒处理过的柱面只有当幽灵驻机时才能解密读出，造成微机硬盘依赖于病毒才能工作的局面。

幽灵病毒的编制者对反病毒专业技术和用户防反病毒的操作习惯有深入的分析了解，采用了多种技术对抗 CPAV、SCAN、CLEAN 等著名软件，还为普通防病毒卡设下了陷井。当怀疑微机染毒时，可用无毒系统软盘启动微机，检查磁盘一些可执行文件长度，若发现有的文件长度增加 3544 字节或其整倍数，可判定为幽灵病毒。另外幽灵病毒在每次开机的时候处理硬盘的两个柱面，硬盘灯要多亮两下，这是幽灵病毒的一个明显特征，微机引导速度比较慢。

一旦发现幽灵病毒就不能再用硬盘引导开机，否则如前所述，每次开机幽灵都会蚕食硬盘两个柱面；也不要试图用单纯恢复主引导区的方法杀除引导型幽灵，因为病毒处理硬盘的数据保存在引导区中，杀毒前必须利用这些数据恢复硬盘。如果不恢复数据就杀除引导区病毒，则有关数据随病毒一起被清除，将造成部分或全部硬盘数据永久性丢失。所以当微机感染幽灵病毒时应停机不用，尽快寻找完善的消毒工具将其杀除。

九、秋水病毒

94 年下半年国内发现了含有"Autumnal Water"字符串的混合型病毒，中译文为秋水病毒。秋水长度 3072 字节，传染可执行 COM、EXE 文件和硬盘主引导扇区。在微机上加载执行含有秋水病毒的外来软件时，病毒首先传染硬盘主引导扇区，方式是把原引导扇区转移到硬盘的 0 柱 0 面 2 扇区，病毒则占据 0 柱 0 面 1 扇区(即主引导区)和 3 到 6 扇区。硬盘染毒后每次开机都加载病毒占据基本内存高端 4K 字节。

秋水修改三个中断地址，分别用于隐藏、传染和自保护。INT13 是磁盘 I/O 中断，BIOS 的磁盘操作都通过 INT13 进行。秋水修改 INT13 地址指向病毒段偏移 0BE8 处，当读取 0 柱 0 面 1 扇区检查时，病毒把保存在 2 扇区的原引导区读出以欺骗用户。DOS 功能调用 INT21 被病毒修改后指向偏移 034F，在列目录和加载文件时传染可执行文件，同时也用于监视开机日期进行破坏。定时器中断 INT8 每秒约发生 20 次，病毒修改 INT8 指向偏移 02EC，在每次中断过程中病毒检测当前 INT21 地址，如不是病毒的地址，就强行把 INT21 地址再改成病毒地址，这是病毒为强赖在内存中而采用的自我保护措施。

秋水的激发日期是 7 月 13 日，病毒截获的 INT21 在入口处先用 AH = 2A 功能获取系统日期，如为 7 月 13 日，就强行干扰键盘使微机不能正常工作。秋水通过列目录和加载文件两种方式传染文件，速度很快，染毒文件都加长 3K 字节，占用大量磁盘空间。由于病毒通过 INT8 调用随时强行修改 INT21 地址，所以在病毒加载后再运行其它正常修改 INT21 的应用软件，例如常用的 dBASE III、VSAFE、GB4 等将不能运行。秋水程序中存在着严重错误，将造成很多 COM 文件染毒后不能运行。

用 DEBUG 观察基本内存 0000 段的中断向量，如果 INT8、INT13 和 INT21 的段地址相同，而且偏移分别为 02EC、0BE8 和 034F，说明秋水病毒已经进驻内存，应立即关机，用无毒系统软盘启动后进一分析磁盘静态病毒的来源。

对怀疑感染秋水病毒的文件可用 DEBUG 调出，检查文件尾部倒数第 1050 个字节起若有字符串“Autumnal Water”，即为秋水的“版权”。感染秋水的 COM 文件第一条指令是 JMP，该指令指出的地址就是原文件尾，从该地址值加 46H 起 5 个单元中保存着原文件的前 5 个字节数据，把它们移到 100H-104H 单元，并根据 JMP 地址把截断病毒后的文件写回磁盘，就杀除了 COM 文件中的病毒。

十、Casper 变形病毒

Casper 原是美国一部卡通片主人公的名子，现在被用来命名一种十分复杂的变形病毒。Casper 病毒被发现后，有人计算出它有上亿种变化，特别在一些产品广告中有说千百亿变化的；也有人对上亿的算法提出质疑。不论是否上亿，Casper 的变化复杂的确是事实。

Casper 的总长度是 1200 字节，其中有 1161 个字节经过加密处理，其余 39 字节则用于对加密部分解密。变形病毒不同于普通加密病毒的地方在于它的解密程序段是千变万化的，可以看一下 Casper 对同一文件两次传染的开头部分：

第一次传染

```
38A5:3F80 B90005          MOV     CX,0500
38A5:3F83 BFA73F          MOV     DI,3FA7
38A5:3F86 90              NOP
38A5:3F87 B8F272          MOV     AX,72F2
38A5:3F8A 2BD8            SUB     BX,AX
38A5:3F8C 3105            XOR     [DI],AX
38A5:3F8E 90              NOP
38A5:3F8F 2BDA            SUB     BX,DX
```

第二次传染

```
38A5:3F80 FC              CLD
38A5:3F81 BFA73F          MOV     DI,3FA7
38A5:3F84 46              INC     SI
```

```
38A5:3F85 B97305        MOV     CX,0573
38A5:3F88 B8E3C6        MOV     AX,C6E3
38A5:3F8B 310D          XOR     [DI],CX
38A5:3F8D 2BDA          SUB     BX,DX
38A5:3F8F 90            NOP
```

如果不事先说明,很难相信它们是同一个计算机程序,它们都是正常的机器语言指令,起着同样的作用。上述变化是 Casper 在传染过程中自动产生的,而非人工修改的变种,再加上病毒加密部分的变异,就造成 Casper 磁盘记录形式上的千变万化。据传 94 年夏季华东地区就有 Casper 的踪迹,但直到 95 年 2 月才随幽灵病毒一起曝光。这时离 Casper 的激发日期 4 月 1 日仅剩一个多月,我国的求真卡和 KILL、KV 等软件迅速应战,都赶在 4 月 1 日前完成了杀除 Casper 病毒的升级。但在另一方面据有关商情部门调查,95 年 4 月 1 日仍有百分之十的用户微机遭到 Casper 病毒的袭击,这一比例是相当可观的。

Casper 是 1200 字节长的文件型病毒,传染 COM 文件。与大多数文件型不同的是 Casper 不驻留内存,在运行一个带毒文件的时候搜寻和传染另一不带毒的文件。由于防病毒卡监测不到病毒驻机,所以不能报告发现病毒,但当病毒企图传染文件的时候多数防病毒卡予以报警。Casper 的破坏作用是 4 月 1 日格式化磁盘。

尽管 Casper 是十分复杂的变形病毒,但它的作用机理却显得很粗糙,它没有隐藏长度变化,所以不论内存是否有毒,只要列目录发现 COM 文件长度增长 1200 字节,就可基本判定染毒。此外在运行写保护软盘文件时,如屏幕莫名奇妙地显示写保护错,则很可能是 Casper 正在传染,而其它很多病毒在软盘写保护时则停止传染。由于 Casper 变化多端,建议尽量采用反病毒工具杀除病毒。

十一、2128 病毒

2128 是 1995 年 2 月份在西北地区首先发现的新病毒,病毒中没有显式字符串,根据长度命名为 2128,KILL 软件对该病毒的命名是 ZGB。

与其它文件型病毒比较，2128 显得长一些，其作用机理也比较复杂。2128 传染可执行 COM 文件和 EXE 文件，每次开机后第一次执行一个带毒文件时，2128 修改 INT21 中断地址，获取并记录系统日期为删除文件作准备，最后利用 INT21 的 31H 调用强占 2368 字节基本内存退出。

被修改的 INT21 地址偏移是 3D9H，病毒监视 4B00 调用，在加载执行 COM 和 EXE 文件时进行传染。病毒加在文件尾部，文件的建立时间秒值被改成 1EH 作为感染标志。一般文件型病毒都是传染磁盘上已经存在的文件，但 2128 却会“无中生有”地制造出带毒的新文件，这是病毒利用 INT21 的 3C 和 3E 两个调用进行传染的结果。3C 的功能是创建一个新文件，LINK 和某些 INSTALL、SETUP 等会用到 3C 功能创建新的文件，2128 从中作乱直接产生带毒文件，具有更大的隐蔽性。在列目录的时侯，对于染毒文件将显示减去病毒长度后的结果以蒙混过关。

2128 的恶性破坏作用表现在 4 月 17 日或者 8 月 17 日开机所运行的任何可执行文件将被删除，同时病毒所控制的列目录程序段中也编入了删除文件的程序。值得注意的是单纯用 DOS 的 41 调用删除的文件可以用 PC 等工具恢复，因此 2128 不满足于单纯 41 删除，而附加了其它技术，使被删除的文件无从救回。除直接破坏作用外，2128 驻机后，如果用户再加载其它合法修改 INT21 的软件，病毒将试图进行拦截，由于病毒编制有误将造成死机。

观察基本内存 0000 段的 INT21 的偏移地址为 03D9H，并且 INT21 段偏移 03DFH 有 CMP BX，9999 指令，表示病毒已经进入内存，应关机用无毒系统软盘启动查找消除磁盘静态病毒。用 DEBUG 调出文件，IP 初值为 100，CS：100 指令为 JMP017E，CS：180 指令为 MOV BX，9999，即可判定感染 2128 病毒，原文件头的 SS、SP、IP、CS 分别保存在病毒的 CS：137、139、13B、13D，病毒长度 850H。

十二、DONG 和 HIDENOWT 病毒

计算机软硬件总是在不断地升级换代，计算机病毒也有升级之说。病毒升级不是简单的变种关系，而是一种病毒较之另一种病毒有了实质性的改变。HIDENOWT 病毒是 DONG 病毒的换代产品。DONG 的兼容性不好，有些文件染毒后在高版本 DOS 下一运行就死机，而 HIDENOWT 改善了 DONG 的兼容性。

DONG 和 HIDENOWT 都是长度为 1757 字节文件型病毒，传染可执行的 COM 和 EXE 文件。微机首次执行含毒文件时，病毒就传染硬盘根目录下的 COMMAND.COM 文件，以后每次开机通过加载 COMMAND.COM 而驻机。病毒占用基本内存高端 7D0H 字节，转换为十进制恰为 2000 字节。对于 640K 基本内存的微机，病毒的段地址是 9F83，修改 DOS 调用 INT21 向量指向 9F83:063F。病毒拦截 INT21 的 11、12、1A 功能，在用户列目录时传染 COM 和 EXE 文件，其传染速度很快，如果不能及时发现消除，会在短时间内传遍整个硬盘，但病毒不传染长度小于 1K 的文件。

DONG 和 HIDENOWT 病毒具有复杂的加密体系，采用封锁键盘和软件措施反跟踪，分析这个病毒的难度较大。病毒驻机后仍有加密和解密操作，从而影响微机运行速度。

十三、IN60 病毒

大多数引导型病毒在传染硬盘主引导区的时候把主引导程序改成病毒引导程序，这些病毒通过与正常引导区比较就能被发现。IN60 则另立门户，采用了很狡猾的手段隐藏自己。IN60 对硬盘主引导程序不做任何修改，而是只改动主引导扇区中分区表的两个数据，使得微机引导过程中读出主引导区后接着读出隐藏在硬盘 0 头 0 柱 2 扇区的病毒，IN60 的引导过程可以从图 8-1 清楚地看出来。

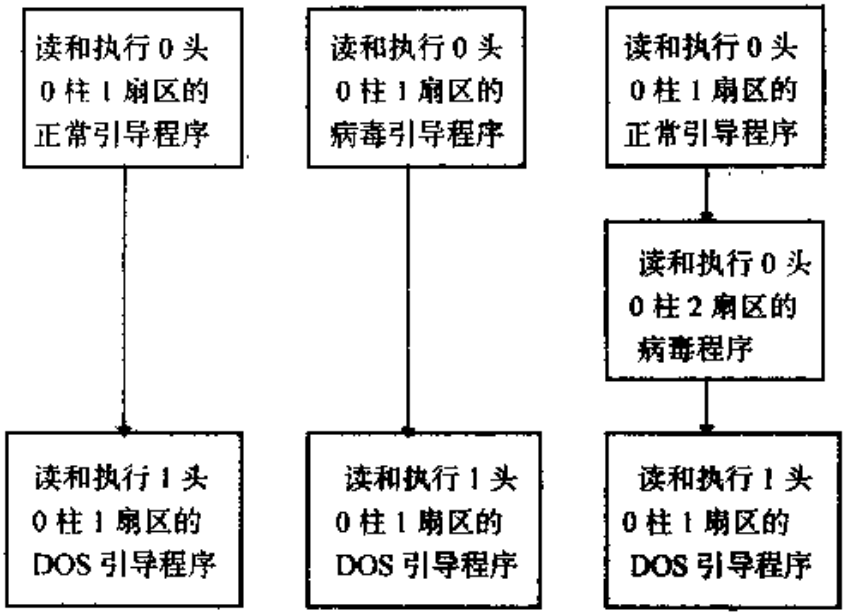


图 8-1　IN60 病毒的引导过程

十四、255 病毒

1995 年 3 季度华东地区新发现了一种引导型病毒，病毒感染引导硬盘引导区后开机(包括冷、热启动)达到 255 次条件下格式化硬盘 0 磁道，故命名为 255 病毒，破坏性很严重。病毒首次传染硬盘主引导扇区是通过带毒的软盘来完成的，如果用户不小心用带毒软盘启动计算机，即使该磁盘不是系统盘，病毒仍然要驻机传染硬盘主引导扇区。当用软盘引导时，病毒程序首先被调至内存 0000:7C00 处执行。病毒先将中断向量 13H 入口地址保存在病毒偏移 1A7H- 1A9H 处，以便在病毒读写扇区时，直接转入该中断。然后读出内存总容量减去 1K，并且计算高端地址，然后将病毒移到高端，通过压栈将控制权交给高端病毒。接着病毒把保存在当前盘的最后一个扇区的原引导记录读到内存 0000:7C00 处。同时读出硬盘的主引导扇区，比较主引导扇区偏移

3AH 处和病毒相同位置的字，若两者相等，说明硬盘已经传染了病毒，不再传染。否则用硬盘分区表覆盖掉病毒的相应部分，并把含硬盘分区表的病毒写回主引导扇区。同时修改 INT 13H 中断，使之指向病毒高端偏移 130H 处，然后转入正常 DOS 引导。

十五、JESSICA 流浪者病毒

Jessica 又名流浪者是长度为 1345 字节的文件型病毒，1995 年夏季在我国出现，它的得名源于病毒的尾部有一段自述：

Dear Jessica:

This is to commemorate our pure and deep friendship whichbegan in R405, PUDY, 1992. My wanderlust comes from the love forfreedom.

Wanderer V1.1 NT.

病毒为了达到传染和破坏的目的，往往需要驻留在基本内存。不同的病毒使用的方法也不尽相同。有的直接利用中断 27H 实现驻留，有的利用中断 21H 的 31H 号功能达到目的。Wanderer 侵占内存并不使用中断，而是直接向基本内存高端传送。这种方法同样也是很多病毒采用的。

JESSICA 是通过执行染有病毒的文件来进驻内存的。当执行染有病毒的文件时，先跳至病毒程序，病毒用 AX = EEEEH 来执行中断 21H，若返回 1234H 说明病毒已经驻留内存，则转入正常程序运行。否则，将 PSP 段偏移 02H 的可用最大内存减去 810H(2064 个)字节，把病毒程序送到高端，同时修改中断 21H，使之指向高端病毒程序段偏移 15BH 处，然后执行正常程序。至此，基本内存高端的 2K 字节便成了流浪者的栖息地，它通过中断 21H 这个通道，不断传染 COM 文件和 EXE 文件，并通过拷盘等方式到处传播。在传染的时候，利用 2AH 功能读文件最后修改时间，判断时间秒值，若高二位为 1，不再传染。即对时间秒值为 1CH 和 1DH 的文件都当做染毒文件，一律放过。这也使得少数时间秒值大于等于 56 秒的文件侥幸逃脱。对尚未感染的 COM 文件若长度小于 E000H(57344) 个字节，且不等于 AC8AH(44170)个字节

时，病毒会附加在文件尾部，同时修改文件的前三个字节指向病毒部分，把原文件的头三个字节放在病毒段偏移 45EH 处。对 EXE 文件修改文件头，将初始代码段 CS 和指令指针 IP 分别指向病毒段和偏移 139H 处，把病毒放在文件后部。最后将文件时间秒值的高三位置 1，作为染毒标志。JESSICA 不隐藏自己的长度，可以通过列目录发现 COM 文件增加了 1345 个字节，对 EXE 文件由于要对原文件以 16 取整，所以增加的长度稍长。

在执行染有病毒的 EXE 文件或病毒驻机情况下执行 EXE 文件时，病毒先读系统时间，若是 8 月 10 日，就会在屏幕上打出“Dear Jessica:....”，干扰用户的工作。病毒的破坏作用是删除 CHKLIST.CPS 和 CHKLIST.MS 文件

十六、DIEHARD 死硬病毒

DieHard 死硬病毒发现于 1995 年春季，“DieHard”是病毒程序解密后在代码尾部出现的字符串，英文的原意是“不易死、很难死”。从病毒程序看，DieHard 的确具有相当高的专业水准。

DieHard 病毒代码长达 4000 个字节，分前后两段分别进行静态加密和动态加密，不同的被感染文件的病毒部分总是不尽相同。DieHard 采用了反跟踪技术，使得经验不足者往往陷入 DieHard 设下的陷阱。DieHard 不仅病毒代码本身长达 4000 个字节，而且驻机后强行占用高端达 9K 字节内存，截获 INT21H 、13H、10H、1H、8H、24H 等多个中断，对系统影响很大。

DieHard 是通过执行带毒的 EXE 文件或 COM 文件进入内存高端的。当染毒文件运行时首先跳到病毒段执行。病毒段偏移 0H—59H 是唯一的一段明码，用来对加密部分进行解密。密钥存放在 96H 处，每次执行病毒将其加 1，使得加密部分变化无穷。这段解密程序将偏移地址 849H—0E7FH 代码解密，这时在尾部会看到病毒的标志“SW DieHard”。对解密后病毒偏移 66H—7dH 处的 24 个字节取反，即为染毒前文件开始处的 24 个字节。DieHard 将前三个字节送回原处，以便

在病毒安装完成后再执行原文件。病毒修改中断 8H 和 1H，用来跟踪中断 21H、10H，获得它们的转移地址，加到病毒程序中，达到以假乱真的目的。然后将可用内存减去 9K(2400H)个字节，计算驻留段值，把病毒代码传至高端，并修改中断 21H 和 10H，使它们分别指向病毒驻留段偏移 98CH 和 0ABEH 处。同时将病毒重新用改过的密钥加密放置病毒驻留段偏移 1400H 处，以便向文件传染。再将病毒驻留段偏移 0d18H 处的 300 个字节全部用 0FF 覆盖掉，再跳至第二段解密程序，对前半部病毒程序解密，然后寻找 COMMAND.COM 文件进行传染，以后每次开机都由 COMMAND.COM 文件引导进驻内存。

DieHard 修改了中断 21H 和 10H，当 DOS 要对文件进行操作时，则转入病毒控制，先判断 COM 文件或 EXE 文件是否已经被感染，若还未感染，就会将病毒驻留段偏移 1400H 处的 4000 个字节强行加到文件的尾部，修改原文件开始的前三个字节，使文件加载时先跳到病毒程序处理。原文件开始的 24 个字节取反放到病毒段偏移 66H 处，以用来判断文件是否被感染。在转入病毒控制时，DieHard 也挪用了中断 0H 和 24H，使得在有除法溢出和严重错误时，先将已经解密的病毒前半部(偏移 97H-848H)重新用未解密的 1497H—1C48H 处的病毒程序覆盖掉，然后才转入正常的处理程序。

当病毒判断计算机在置 VGA 下 320×200 的 256 色显示模式时，会在屏幕上显示它的标志“SW”。由于要在 DS:1200H 处置 64 个字节的调色板值，有时会造成执行程序数据有错不能正确执行，甚至死机。DieHard 在执行 INT 21H 的 3D 功能时(打开文件)，要检测系统时间，若是星期二且不是 3、11、15 号或 28 号时，会在屏幕上打出“SW Error”，造成死机。且由于每次调用中断 21H 和 10H 时，病毒都要进行一次解密过程，使运行速度大大降低。

DieHard 不仅传染 COM 文件和 EXE 文件，而且攻击重要的以 PAS 和 ASM 为扩展名的源文件。DieHard 先将原文件的前 256 个字节移到文件尾部，然后在文件头加入非法的小段程序。

DieHard 虽然隐藏得很深，但还是有它的症候的。如果发现机器运

行速度明显变慢，且 COMMAND.COM 增加了 4000 个字节，可以用 debug 将中断向量表调出，若 21H 和 10H 的段值相同，且偏移地址分别是 98CH 和 0ABEH，则 DieHard 已经驻机。重新用干净的系统盘启动，向硬盘上拷贝 COMMAND.COM。

附录　国内已发现的主要计算机病毒特性表

（截止 1995 年 11 月）

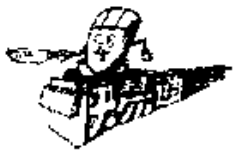
A Infects Fixed Disk Partition Table
9 Infects Fixed Disk Boot Sector
8 Infects Floppy Diskette Boot
7 Infects Overlay Files
6 Infects EXE Files
5 Infects COM files
4 Infects COMMAND.COM
3 Virus Installs Self in Memory
2 Virus Uses Self-Encryption
1 Virus Uses STEALTH Techniques

Virus name	1	2	3	4	5	6	7	8	9	A
1. Ping Pong	.	.	*	.	.	.	.	*	*	.
2. Ping Pong 8024	.	.	*	.	.	.	.	*	*	.
3. Stoned	.	.	*	.	.	.	.	*	.	*
4. Alameda	.	.	*	.	.	.	.	*	.	.
5. Michelangelo (3.6)	.	.	*	.	.	.	.	*	.	*
6. Bloody	.	*	*	.	.	.	.	*	.	*
7. Bloody-B	.	*	*	.	.	.	.	*	.	*
8. Bloody-C	.	*	*	.	.	.	.	*	.	*
9. Bloody-D	.	*	*	.	.	.	.	*	.	*
10. Bloody-E	.	*	*	.	.	.	.	*	.	*

11. Azusa [2708]	.	.	*	.	.	.	.	*	.	*
12. 2708-B	.	.	*	.	.	.	.	*	.	*
13. 2708-C	.	.	*	.	.	.	.	*	.	*
14. 2709	.	.	*	.	.	.	.	*	.	*
15. Brain	.	.	*	.	.	.	.	*	.	.
16. Korea	.	.	*	.	.	.	.	*	*	.
17. GuangZhou 1	.	*	*	.	.	.	.	*	.	*
18. GuangZhou 2	.	*	*	.	.	.	.	*	.	*
19. Be	.	.	*	.	.	.	.	*	.	*
20. Chinese Bomb	.	*	*	*	.	.	.	.	.	.
21. Chinese Bomb-B	.	*	*	*	.	.	.	.	.	.
22. Fu Manchu	.	.	*	.	*	*	*	.	.	.
23. 1701/Cascade	.	*	*	*	*	.	.	.	.	.
24. Yank Doodle	.	.	*	.	*	*	.	.	.	.
25. Yank Doodle-B	.	.	*	.	*	*	.	.	.	.
26. Keypress	.	.	*	*	*	*	.	.	.	.
27. 1575/1591	.	.	*	*	*	*	.	.	.	.
28. Liberty	.	.	*	*	*	*	*	.	.	.
29. W-13	.	.	.	.	*	.	.	.	.	.
30. Sunday	.	.	*	.	*	*	*	.	.	.
31. Vienna	.	.	.	.	*	.	.	.	.	.
32. Jerusalem	.	.	*	.	*	*	*	.	.	.
33. Oropax	.	.	*	.	*	.	.	.	.	.
34. Disk Killer	.	.	*	.	.	.	.	*	*	.
35. V2000	.	.	*	*	*	*	*	.	.	.
36. Dark Avenger	.	.	*	*	*	*	*	.	.	.
37. Travel-A	.	.	*	.	*	*	.	.	.	.
38. Travel-B	.	.	*	.	*	*	.	.	.	.
39. Travel-C	.	.	*	.	*	*	.	.	.	.

40. Flip . * * * * * * . . .
41. Flip-B . * * * * * * . . .
42. Nflip . * * * * * * . . .
43. Ma . * * * * * . . . .
44. 1554 . . * * * * . . . .
45. N64 . . * * * * . . . .
46. Gene . * * . . * . . . .
47. Century . * * * * * . . . *
48. Dong . . * * * * . . . .
49. Libin-A . * * * * * . . . .
50. Libin-B . * * * * * . . . .
51. Libin-C . * * * * * . . . .
52. Dir-2 * . * * * * . . . .
53. 4096 . . * * * * . . . .
54. Taiwan3 . * * * * * . . . .
55. Taiwan4 . * * * * * . . . .
56. Invader . . * * * * . . * .
57. Plastique . . * * * * . . * .
58. 1704 . * * . * . . . . .
59. Nsunday . . * * * * . . . .
60. Story . . * . . * . . . .
61. 848 (Qian) . . * * * . . . . .
62. Poor_Man . . * * * . . . . .
63. Big-ball . * * * * * . . . .
64. Genb . . * . . . . * . *
65. Genp . . * . . . . * . *
66. Torch . . * . . . . * . *
67. loa Duong . . * . . . . * * .
68. In-70 . . * . . . . * . *

69. Lucky	.	.	*	.	.	.	.	*	.	*
70. Democracy	.	.	*	*	*	*	.	.	.	.
71. Paralyze eyes	.	*	*	*	*	*	.	.	.	.
72. Pao	.	*	*	*	*	.	.	.	.	.
73. Solano	.	.	*	*	*	*	.	.	.	*
74. Custom	.	.	*	.	.	*	.	.	*	*
75. 2708-D	.	.	*	.	.	.	.	*	.	*
76. Stone-B	.	.	*	.	.	.	.	*	.	*
77. Stone-C	.	.	*	.	.	.	.	*	.	*
78. Genb-B	.	.	*	.	.	.	.	*	.	*
79. Girl	.	.	*	.	.	.	.	*	*	.
80. Anti_Tel	.	.	*	.	.	.	.	*	.	*
81. Dabi	.	*	*	*	*	*	.	.	.	.
82. Dabi_A	.	*	*	*	*	*	.	.	.	.
83. 888	.	*	*	*	*	*	.	.	.	.
84. Fish	.	.	*	.	.	.	.	*	.	*
85. Basic	.	.	*	.	.	.	.	*	.	*
86. Genb_C	.	.	*	.	.	.	.	*	.	*
87. EXEBug[Swb]	.	.	*	.	.	.	.	*	.	*
88. Stone-D	.	.	*	.	.	.	.	*	.	*
89. Stone-E	.	.	*	.	.	.	.	*	.	*
90. SUST	.	.	*	.	.	.	.	*	.	*
91. FORM	.	.	*	.	.	.	.	*	*	.
92. 623	.	.	*	*	*	.	.	.	.	.
93. Mummy(FamE)	.	*	*	.	.	*	.	.	.	.
94. EEACER	.	.	*	.	.	.	.	*	.	*
95. DA01	*	*	*	*	*	*	.	.	.	.
96. BAI	.	.	*	*	*	*	.	.	.	.
97. Selfex	.	.	*	*	*	*	.	.	.	.



98. INT60	. . * . . . . * . *
99. ExeBug1[ExBg1]	. . * . . . . * . *
100. Azusa_D	. . * . . . . * . *
101. Docter	* * * * * * . . . .
102. V_44C	. . * * * * . . . .
103. Gene2	* * * * * * . . . .
104. Stone-F	. . * . . . . * . *
105. Stone-G	. . * . . . . * . *
106. ZRK	. * * . * * . . . .
107. WOLF	. * * * * * . . . *
108. MULINT	. * * * * * . . . .
109. 2803	. . * . . * . . . .
110. Alfa	. . * * * * . . . *
111. 1367	. . * * * * . . . .
112. INT60_B	. . * . . . . * . *
113. Bupt	. . * . . . . * . *
114. Stone-H	. . * . . . . * . *
115. 2062	. * * * * * . . . .
116. Ming	. . . * * . . . . .
117. ZeroBug	* . * * . . . . . .
118. AntiExe	. . * . . * . * . *
119. Genp/Genb-31R	. . * . . . . * . *
120. BackForm	* . * * * * . . . .
121. Water	. . * . * * . . . *
122. Mei	. . * * * * . . . .
123. Birthday	. * * * * . . . . .
124. Die_hard	. * * * * * . . . .
125. 934	. . * * * . . . . .
126. PRGKill	. . * * * . . . . .

127. One_Half	*	*	*	*	*	*	.	.	.	*
128. Hidcnowt	.	*	*	*	*	*	.	.	.	.
129. BOOT-437	.	.	*	.	.	.	.	*	*	.
130. Denzuko	.	.	*	*	*	*	.	.	.	*
131. Jushi	.	.	*	.	.	.	.	*	.	*
132. B1	.	.	*	.	.	.	.	*	.	*
133. Junkie	.	*	*	*	*	.	.	*	.	*
134. Monkey	.	*	*	.	.	.	.	*	.	*
135. 2707	.	.	*	.	.	.	.	*	.	*
136. Casper	*	*	.	*	*	.	.	.	.	.
137. AAV	.	.	*	.	*	*	.	.	.	.
138. Parity	.	.	*	.	.	.	.	*	.	*
139. Stone. Empire	.	*	*	.	.	.	.	*	.	*
140. Leandro	.	.	*	.	.	.	.	*	.	*
141. ZGB	.	.	*	*	*	*	.	.	.	.
142. 1167	.	.	*	*	*	*	.	.	.	.
143. Vtech	.	*	*	.	.	*	.	.	.	.
144. Genp/Genb005	.	.	*	.	.	.	.	*	.	*
145. 768(November_17th)	.	.	*	*	*	*	.	.	.	.
146. Lyceum(930)	.	.	*	*	*	*	.	.	.	.
147. Angelina	.	*	*	.	.	.	.	*	.	*
148. Keypress1	.	.	*	*	*	*	.	.	.	.
149. Flame	.	.	*	.	.	.	.	*	.	*
150. 1701/Cascade-A	.	*	*	*	*	.	.	.	.	.
151. Stone-16	.	.	*	.	.	.	.	*	.	*
152. Dinamo	.	.	*	.	.	.	.	*	.	*
153. CHINA	.	.	*	*	*	.	.	.	.	.
154. BUPT9146	.	*	*	.	*	*	.	.	.	.
155. HK. 2358	.	*	*	*	*	*	.	.	.	.

156. Jessica	.	*	*	*	*	.	.	.	.	
157. RS. Y	.	*	*	.	.	.	.	*	*	.
158. Nice_Day	.	*	*	.	.	.	.	*	.	*
159. New_Wolf	.	*	*	*	*	*	.	.	.	*
160. Stone-I	.	.	*	.	.	.	.	*	.	*
161. NewDemocracy	.	*	*	*	*	*	.	.	.	.
162. Flip5	.	*	*	*	*	*	*	.	.	.
163. BOOTEXE	*	.	*	.	.	*	.	*	*	.
164. Vacsina	*	.	*	*	*	*	.	.	.	.
165. Natas	*	*	*	*	*	*	.	*	.	*
166. Lighting	.	.	.	*	*	.	.	.	.	.
167. Russian-flag	.	.	*	.	.	.	.	*	.	*
168. Wanderer	.	.	*	*	*	*	.	.	.	.
169. Baby	.	.	*	.	.	*	.	.	.	.
170. Mulint3	.	*	*	*	*	*	.	.	.	.
171. 891	.	.	*	*	*	*	.	.	.	.
172. Mummy10	.	*	*	.	.	*	.	.	.	.
173. Doglas	.	*	*	*	*	*	.	.	.	.
174. AAV-2	.	.	*	.	*	*	.	.	.	.
175. CVEX3	.	.	*	*	*	*	.	.	.	.
176. RMB	.	.	*	.	.	.	.	*	.	*
177. Genb-D	.	.	*	.	.	.	.	*	.	*
178. Tremor	*	*	*	*	*	*	.	.	.	.
179. Tai-pan. 438	.	.	*	.	.	*	.	.	.	.
180. Parity-A	.	.	*	.	.	.	.	*	.	*
181. 1898	*	*	*	*	*	*	.	.	.	.
182. Apr-4th. 751	.	.	.	*	*	.	.	.	.	.
183. Billiard. 2658	*	*	*	.	*	*	.	.	.	.
184. ExeBug2	.	.	*	.	.	.	.	*	.	*